Author:
Raffaelli, Francesco

Title:
Quantum random number generators in integrated photonics

Quantum Random Number Generators in Integrated Photonics

by

Francesco Raffaelli

A thesis submitted in partial fulfillment for the degree of

Doctor of Philosophy

in the Faculty of Science

School of Physics

December 2018

Abstract

Random numbers find applications in a range of different fields, from quantum key distribution and classical cryptography to fundamental science. They also find extensive use in gambling and lotteries. By exploiting the probabilistic nature of *Quantum Mechanics*, quantum random number generators (QRNGs) provide a secure and efficient means to produce random numbers. Most of the quantum random number generators demonstrated so far have been built in bulk optics, either using free space or fibre-optic components. While showing good performance, most of these demonstrations are strongly limited in real life applications, due to issues such as size, costs and the manufacturing process.

In this thesis I report the demonstration of three different QRNGs based on integrated photonics. First, I demonstrated a QRNG based on homodyne measurement of optical vacuum states on a Silicon-on-insulator (SOI) chip. Second, I developed a SOI QRNG based on phase fluctuations from a laser diode. In these two schemes all the optical and opto-electronic components, excluding the laser, were integrated onto a silicon-on-insulator device. These schemes, being built on a silicon-on-insulator chip are potentially CMOS compatible and pave the way for being integrated onto other more complex systems. These QRNGs showed Gbps generation rates and passed the statistical tests provided by NIST. Third, I report the preliminary study of a QRNG based on homodyne measurement of optical vacuum states onto a Indium Phosphide (InP) chip. In this third experiment, all the components, including a laser diode, were monolithically integrated in the same chip, which provide a great advantage in terms of the overall size of the optics of the device.

Declaration of Authorship

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's Regulations and Code of Practice for Research Degree Programmes and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

Signed: _____

Date: _____

Acknowledgements

First, I would like to thank Jonathan, for the opportunity to pursue my PhD and for guiding my research in these four years. Thank you for giving me the chance to follow my curiosity and for pushing me to get the best out of my research.
Thank you, Dylan, for being so helpful, always ready to answer my questions. I would like to thank Giacomo for sharing a big part of my research in these years. The daily loud discussions about science and food, which kept annoying our colleagues in office 1.25, gave me the chance to learn a lot.
Thank you, Phil and Jake, for sharing the QRNG experiments and for the useful discussions and tips. I should also thank Jake for organising the weekly 5-a-side football – much needed and very good fun. I would like to thank all the other QETLabs colleagues, in particular the continuous-variable team for the very enjoyable discussions and daily help.
A special thank goes to Magnus Loutit, for introducing me to the *Dark Magic* of high-speed electronics and for answering any silly question that would come to my mind. Your advice has been fundamental for my research. A special thanks to Andy Murray, because without good wire-bonds it is impossible to do any integrated photonics whatsoever – thank you for rescuing my chips so many times. I also want to thank all the QETLabs admin staff, for helping me solve any and every query I had.
I want to thank my parents and my brothers, for the support you have always demonstrated. Finally, the biggest thanks is for the witty Harriet, my wonderful wife.

Published Manuscripts (peer-reviewed)

F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. F. Matthews, "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers," *Quantum Science and Technology*, vol. 3, no. 2, p. 025003, 2018, DOI: `https://doi.org/10.1088/2058-9565/aaa38f`.

F. Raffaelli, P. Sibson, J. E. Kennard, D. H. Mahler, M. G. Thompson, and J. C. F. Matthews, "Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip," *Optics Express*, vol. 26, pp. 19730–19741, 2018, DOI: `https://doi.org/10.1364/OE.26.019730`.

Presentations

Posters

F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, J. C. F. Matthews, "An On-chip Homodyne Detector for Generating Quantum Random Numbers and Measuring Coherent States", QCrypt 2017, Cambridge, UK, 2017.

G. Ferranti, F. Raffaelli, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, J. C. F. Matthews, "An On-chip Homodyne Detector for Quantum Technologies" BQIT2017, Bristol, 2017.

G. Ferranti, F. Raffaelli, D. H. Mahler, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, J. C. F. Matthews, "On-chip Homodyne Tomography of single photons generated in a silicon micro-ring resonator", Young Scientists Conference, Bristol, 2016.

Talks

F. Raffaelli et al., "High performance quantum random number generators in silicon photonic", Photon 2018, Aston University, Birmingham (UK), 2018.

F. Raffaelli et al., "On-chip Quantum Random Numbers based on vacuum states", School of Physics, University of Bristol, Postgraduate Conference, 2016.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Random numbers are central to science and technology. They are an important resource in simulations and are a necessary requirement in classical and quantum cryptography. Often, generation of random numbers is achieved by means of algorithms usually based on number theory. This kind of random numbers generator (RNG) is called a pseudo-RNG [1]. However, as Von Neumann said:

"Anyone who attempts to generate random numbers by deterministic means is, of course, living in a state of sin.".

This quote expressed the simple and yet remarkable fact that any algorithm that tries to generate a set of random numbers, for the simple fact that it is an algorithm, and thus reproducible, will fail its aim. Starting from this simple observation, the scientific community realised that in order to produce secure random numbers a solid alternative was to generate randomness from a physical *random* process, through a true random number generator (TRNG). A simple TRNG can be obtained by exploiting the electronic noise in electronic circuits. In this case the noise generated by a current flowing through a resistor or a diode could be amplified and digitized, providing a random signal [2]. Alternatively, some complex biological processes can be used to generate random numbers [3], which are however strongly limited in terms

of achievable generation rate. Other TRNGs are reported in Table 1.1. [4–8]. Unfortunately, all the aforementioned methods suffer from two main limitations. Often, the randomness is not due to intrinsic random processes, but it is due to processes whose complexity make them appear as random[1]. Therefore the randomness is not based on intrinsic randomness but rather on ignorance about the physical processes underlying the RNG. Moreover, as can be observed from Table 1.1, their generation rate is limited to the Mbps regime. An exception is the RNG used by Intel in their integrated processors, which can produce raw bit-strings at the Gbps rate (where although the ultimate source of randomness is still the thermal noise of integrated electronics components).

Physical Principle	References	Generation Rate
Thermal noise in electronic circuits	[2]	1.4 Mbps
Biometric parameters	[3]	low
Chaotic systems	[4]	1 Mbps
Free running oscillators	[5]	0.5 Mbps
RS-NOR metastable latch	[6, 7]	3 Gbps
Thermal noise in integrated oscillators	[8]	30-50 Mbps

TABLE 1.1: ***List of different hardware-based random numbers generators***. *Random number generators based on various physical non-quantum processes.*

To face these limitations, quantum random number generators (QRNGs) based on the nature of *Quantum Mechanics*, an intrinsically probabilistic theory, attracted

[1]In some cases, such as [2], the random bits are generated by a combination of thermal noise, Johnson noise and shot-noise. Electronic shot-noise is an intrinsic quantum effect, whose description is not deterministic and indeed intrinsically random. However it is very difficult to isolate the different sources of noise.

the interest first of scientists and eventually of industry[2].

The first proposals of a *quantum* random number generator were suggested by taking advantage of the probabilistic nature of radioactive decay in atoms [12]. However this scheme suffers from some fundamental and practical issues. On one hand, the low rate of decay sets a limit on the maximum achievable rate. On the other hand, the radioactive processes are intrinsically harmful, requiring a careful design to be integrated into other systems [1]. A more practical solution was to take advantage of the quantum nature of light[3]. Optical QRNG have many features that make them very appealing among all other RNGs. First, optical processes are characterized by high speed, which naturally entails high generation rates. As can be observed by a comparison between Table 1.1 and 1.2, optical QRNG are generally faster than TRNG. This is because high efficiency detection of coherent optical fields can be easily performed at GHz rates, while detection of single photons can be achieved at tens MHz. Second, optical quantum fields can be generated, manipulated and detected with high fidelity, which makes it easy to monitor the physical processes to detect for possible failures of the devices. It is worth noting here that many TRNG based on electronic noise could be considered as *quantum*, given that the electronic shot noise, which is due to the granularity of electrical charges and which is therefore a purely quantum effect, contributes substantially to the overall noise. However, this sort of TRNG cannot be classified as a QRNG because there is no efficient way of isolating the quantum contribution, which is intrinsically random, from the remaining classical chaotic contributions. Third, optical QRNG are based on quantum optics which is a well-established theory that enables a detailed theoretical description of the processes involved, providing a powerful tool to estimate the generated randomness. Particularly interesting are those situations where the RNG is left entirely or partially *untrusted*. By taking advantage of theoretical tools such

[2]ID Quantique in 2001 developed *Quantis*, the first commercial QRNG based on quantum photonics [9]. This was followed more recently by a commercial QRNG produced by Quintessence Labs [10]. Interestingly, ComScire has been commercialising QRNGs based on electronic shot-noise from integrated electronic circuit for almost 20 years [11]. A list of commercially available QRNGs can be found in [1].

[3]Other valid techniques based on electronic systems have been recently developed [11], but they will not be discussed in this introduction. They provide a valuable alternative to optical QRNGs achieving high generation rates in devices with very small form factors.

as Bell's Inequality [13, 14], it is possible to generate randomness without relying on knowledge about the physical device, but simply by looking at the outcomes of the measurements. In this case QRNGs show their superiority compared to other kinds of RNG, providing a means to generate random numbers without having full control of the device itself. This seems very relevant when high-quality random numbers are required in real-world applications and only partial control of the randomness source is achievable. Finally, a feature that makes optical QRNGs appealing is that they are built with the same technology of classical and quantum optical communication systems. Therefore optical QRNGs can by directly integrated into any optical system that requires random numbers, for example cryptographic systems.

In Table 1.2 a list of relevant optical QRNGs is reported. The first optical QRNG was proposed by Rarity et al. [15]. In this scheme, a strongly attenuated beam was sent through a beam splitter. Two single photon detectors were placed at the output of the beam splitter. Referring to Fig. 1.1, a photon detected by D_0 would be recorded as a "0" while a photon detected by D_1 would be detected as a "1". In this way, a sequence of perfectly random bits was experimentally generated for the first time in [16]. In the following decade many implementations taking advantage of similar schemes were proposed and implemented. QRNG based on time arrival statistics of photons have been demonstrated [17–19]. These schemes exploit the intrinsic statistics of light, either by detecting precise time of photon detection or by recording the time between arrival of photons at a detector. Another widely used technique is based on counting the number of photons generated by either a thermal or coherent light source that can be detected within a time window [20, 21]. However, despite being robust and very reliable, all these schemes suffered for low generation rates, limited to tens of Mbps. This is mainly due to the dead time that characterises single photon detection.

A valid solution to enhance the generation rate was found in the continuous-variable framework of quantum optics. In 2010, Gabriel et al. demonstrated a method based on homodyne detection[4] and measurements of optical vacuum states [23, 24]. From

[4]See [22] for a review on homodyne detection.

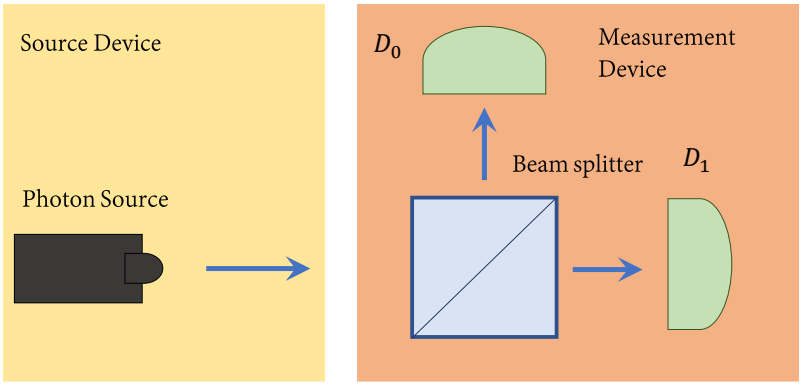

FIGURE 1.1: ***QRNG based on discrete variables.*** *Here we report a scheme of an optical QRNG based on discrete variable. A light source generates a weak beam, directed to a balanced beam-splitter. Ideally, the photons will have a 50% probability of being either transmitted or reflected. A click on detector D_0 will be recorded as a 0, while a click on D_1 will be detected as a 1. Therefore, a perfectly random sequence of 0s and 1s will be generated.*

this first experiment, many demonstrations of the scheme have been proposed [25–28], recently reaching a raw key generation rate of 17 Gbits/s [29, 30] and reaching real-time generation rates up to 6 Gbps [31]. In 2010, another experiment showed that high rates can be achieved by taking advantage of phase fluctuations intrinsic to light generated by laser diodes [32]. This idea was further developed to push the bit generation to higher rates [33], at first up to 68 Gbps [34] and more recently beyond 100 Gbps [35]. In 2011 a similar approach to [32] was proposed. In this case, the random phase fluctuations were achieved by modulating the laser diode in order to obtain a train of pulses, and by interfering subsequent pulses. Because the relative phase between two different pulses is random, by interfering them, the resulting optical intensity is random [36]. This technique was optimised in 2014 to achieve a 43 Gbps generation rate [37]. Another technique based on amplified spontaneous emission (ASE) was first performed in [38] and many variations of the scheme have been demonstrated later on, as for example in [39].

All the experiments cited so far, while achieving important results in terms of generation rates, have been performed either in free space or fibre optics. This fact carries a few limitations. First, the bulk components suffer from phase instabilities and therefore active stabilisation often become necessary in bulk QRNGs. Second,

the size of the components, together with their cost, strongly limits their deployment in real world applications. For this reason in the recent years scientists started looking into ways of making QRNG more compact and practical. In 2014, Sanguinetti et al. demonstrated a QRNG integrated in a camera of a smartphone [40]. In 2016 Abellan et al. [41] showed a high rate QRNG integrated into an Indium Phosphide optical microchip based on a variation of the scheme described in [36] and [37]. At the time of writing this thesis, other demonstrations of integrated or partially integrated QRNGs have been reported. Ref. [42] showed that the scheme in [36] and [37] could be implemented also in the Silicon-on-Insulator platform. In [43], using a Lithium Niobate multipath beam-splitter, a multiplexed system of seven homodyne detector was reported, where both laser source and photodiodes are off-chip, while the integrated multimode beam-splitter was built in Lithium Niobate.

During my Ph.D I focused on the development of continuous-variable[5] QRNG in integrated photonics. On one hand, working in continuous-variable allows the use of standard lasers as sources, and photodiodes for the manipulation and measurement of the quantum states. On the other hand, integrated linear optics components as well as integrated photodiodes are readily available in many integrated platforms, enabling the manipulation and detection of light on chip. Exploiting the continuous-variable regime in integrated devices brings together the advantage of simple components used in continuous-variable and ultra-compact footprint of the integrated devices. Our integrated QRNGs show the potential of monolithic integration within more complex systems, such as integrated QKD terminals, as well as stand-alone, compact high-rate sources of random numbers.

[5]In this thesis I will refer to continuous-variable (CV) as a framework where no highly non-classical states nor single photon detectors are involved. This is to include the phase fluctuations based QRNG in this definition. However, we note that there is a substantial difference between the quantum shot-noise measured in Chapter 3 and the phase noise measured in Chapter 4. The first relies on a well developed theoretical framework of the phase-space description of quantum optics that allows a rigorous security analysis of this kind of QRNG. The second is based on a more empirical approach, where the assumption about the *quantumness* of this QRNG is derived by the fact that spontaneous emission is a physical phenomenon that can be described only with a fully quantum mechanical description of the interaction between atom and EM field.

1.1 Thesis Outline

Chapter 2 is a background chapter where I describe the main experimental and theoretical tools used in this thesis. In Chapter 3 I report the design and characterisation of a silicon-on-insulator integrated homodyne detector, used to characterise coherent states and generate random numbers at Gbps rate. We were able to demonstrate that our homodyne detector has the right specifications to measure quantum states on an integrated platform and when measuring optical vacuum states, can be used to generated random numbers at high speed. In Chapter 4 I demonstrate the generation of high rate quantum random numbers based on laser diode phase fluctuations onto a SOI device. In Chapter 5 I report the preliminary studies of a homodyne detector integrated onto a InP chip, where all the optics, including the laser diode, are integrated onto the same device. In Chapter 6 I describe in more detail the development of the transimpedance amplifiers used in Chapter 3, 4 and 5.

Physical Principle	References	Gen. Rate	Issues
Path/Polarisation	[15, 16]	Mbps	-Unbalanced detection -Detector dead time
Time of arrival	[17–19]	Mbps	-Detector dead time -Timing precision
Photon number statistics	[20, 21]	Mbps	-Detector dead time -Photon number counting
Vacuum fluctuations	[24–26]	Gbps	-Electronic noise -Post-processing
Laser phase noise	[32–34]	Gbps	-Electronic noise -Post-processing
Laser phase diffusion	[36, 37, 41]	Gbps	-Pulse repetition rate -Post-processing
Amplified Spontaneous Emission	[38, 39]	Gbps	-Sampling/ADC -Post-processing

TABLE 1.2: ***List of different techniques to generate quantum random numbers.*** *List of common QRNGs based on different physical principles. For each method the order of the achievable generation rate and the main experimental issues are reported along with the most significant demonstrations.*

Chapter 2

Background

In this chapter I will give a background description of the main experimental and theoretical tools used during my PhD and reported throughout my thesis. In Section 2.1 I will describe the main integrated photonics components available in the Silicon-on-Insulator and Indium Phosphide platforms. In Section 2.2 I will introduce the mathematical tools for linear optics, such as beam-splitters, phase-shifters and Mach-Zehnder interfermeters. In Section 2.3 I will briefly introduce the Wigner quasi-probability distribution (or Wigner function), particularly for coherent states characterised in Chapter 3. In Section 2.4 I will discuss some concepts related with *Quantum Random Numbers Generators* (QRNGs), by discussing the concept of randomness in quantum mechanics. I will also describe the main building blocks of a QRNG: source device, measurement device and randomness extractor. I will describe with more details the concept of randomness extraction, common to the three experiments performed. I will leave to each chapter the details of source and measurement device. Finally, I will discuss the statistical hypothesis tests based on P-values, as this technique is present in the NIST statistical tests suite, used to test our integrated QRNGs.

2.1 Integrated Photonics

In the last 30 years integrated photonics developement and capability have seen an exponential growth, due to the possibility of building complex, scalable, monolithic and highly reproducible devices at low costs. Nowadays, most of the building blocks necessary to perform protocols based on optics can be integrated into single microscopic devices. In the last ten years, starting from the paper of Politi et al. [44], integrated photonics has found applications also in the fields of Quantum Optics and Quantum Information [45, 46]. This enabled the reduction of the complexity of the systems to a level out of reach in bulk optics. In this section I describe the main components available in integrated platforms. The integrated optics components described in this section are present both in the SOI and InP platforms. While the specifications in these two platforms are in general different, the working principle is the same. Therefore, where possible, I will provide a general description that can be applied both to SOI and InP.

2.1.1 Waveguides

In integrated photonic devices, the most fundamental component is the waveguide [47]. Similar to optical fibres, light travels confined in optical channels. Depending on the shape and size, different kinds of integrated waveguides are available. In particular, confinement of light can happen in 1D (planar/slab waveguides) and 2D (strip/rib waveguides). Different types of waveguides are reported in Fig. 2.1.

The general condition for confinement is having a high refractive index core surrounded by a cladding with a lower refractive index. Snell's Law says that

$$n_{core} \sin\theta_{core} = n_{cladd} \sin\theta_{cladd}, \tag{2.1}$$

where we consider the situation where $n_{core} > n_{cladd}$. As shown in Fig. 2.2, the situation where there is no light propagation in the cladding can be expressed as $\theta_{cladd} = \pi/2$.

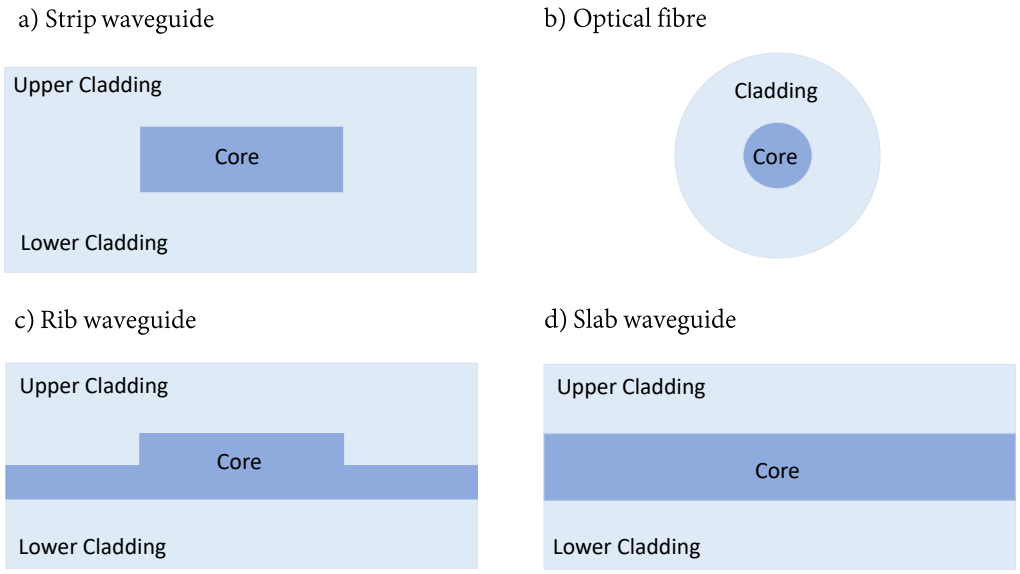

FIGURE 2.1: ***Different types of waveguides.*** *a) Strip waveguide: square shaped waveguide with a well defined height and width b) Optical fibre: characterised by a circular core. c) Rib waveguide: a wider section is deeply etched, while a central section is partially etched. d) Slab waveguide: planar waveguide where the confinement is present just in one direction.*

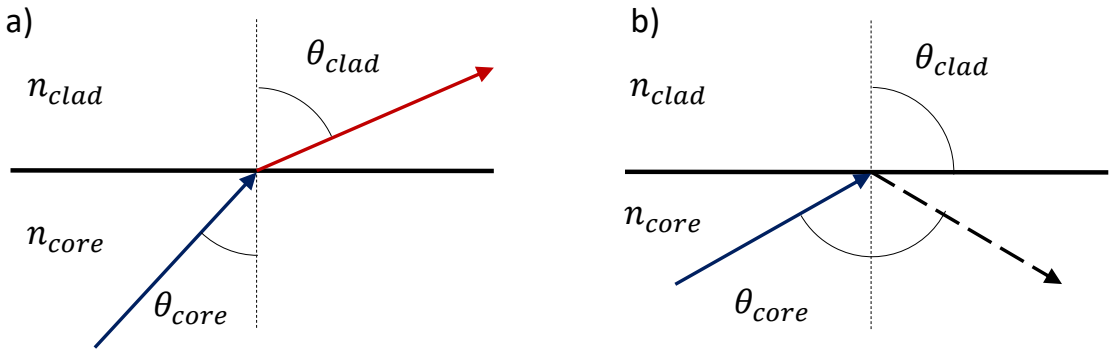

FIGURE 2.2: ***Internal Reflection.*** *Example of deflection and total internal reflection. a) The light in mediums with different refractive indexes is deflected at different angles. b) The light, propagating at an angle greater than a critical angle is constrained inside the glass due to the total internal reflection.*

Here, the confinement is due to a core with higher refractive index than the external cladding. Therefore Eq. 2.1 becomes,

$$\theta_{core} = \sin^{-1} \frac{n_{cladd}}{n_{core}}, \tag{2.2}$$

and θ_{core} is called *critical angle*. For $\theta \geq \theta_{core}$ the light is confined within the higher index region.

2.1.2 In/Out Optical Coupling: Grating Couplers

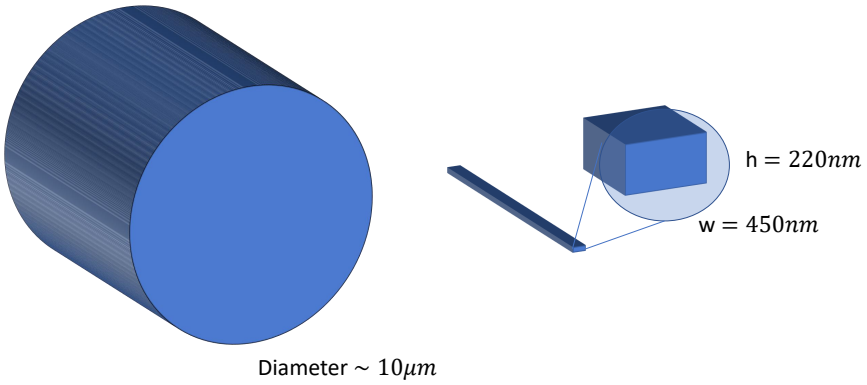

FIGURE 2.3: ***Comparison between the core of an optical fibre and integrated waveguide.*** *In this figure we sketch the core of a single mode optical fibre working at 1550 nm and the section of a single mode integrated waveguide (SOI). The figures are in scale.*

One of the main issues when working with integrated photonics is to couple the light from the optical fibres to the integrated device. Even though many components can be integrated on a single monolithic device, often the laser source is off-chip and it is therefore connected to the chip via optical fibres. Moreover, in SOI as well as in InP, high efficiency single photon detectors are not available yet. Therefore coupling the light off-chip is sometimes necessary also for the detection process.

Here the main problem arises, as the size of the integrated waveguides is approximately one order of magnitude smaller than the core of a standard single mode optical fibre, as shown in Fig. 2.3. Two main methods are used to couple the light

in/out the photonic microchips. They are the horizontal edge coupling [48], and the vertical coupling [49]. The latter is often preferred as vertical coupling can be realised everywhere above the area of the chip. Contrarily, edge coupling can be performed just on the edges of the chip, reducing the number of connections achievable. In Fig. 2.4 a scheme of a grating coupler and an optical fibre is depicted. The grating coupler is characterised by a Bragg grating and a taper, shown in Fig. 2.5, to adapt the different size of waveguide and optical fibres. The angle between the fibre and the grating coupler is chosen to obtain constructive interference inside the Bragg grating. As described in [50], if the light is injected into the waveguide from above the chip, the phase-matching condition for coupling into the chip is

$$\beta_{gr} = k_0 n_1 \sin\theta, \tag{2.3}$$

where n_1 is the refractive index of the air (or cladding), θ is the incidence angle between the fibre and the normal to the chip and β_{gr} is the propagation constant inside the grating. β_{gr} is given by

$$\beta_{gr} = \beta_{wg} - \frac{2\pi}{\Lambda}, \tag{2.4}$$

where β_{wg} is the propagation constant due to the waveguide and Λ is the pitch of the grating. The second term is due to the refractive index modulation introduced by the grating. We observe that without the grating that reduces the overall propagation constant, the propagation inside the chip would not be possible because

$$\beta_{wg} \equiv k_0 n_{eff} > k_0 n_1, \tag{2.5}$$

where n_{eff} is the effective refractive index of the waveguide. Given that $k_0 = \frac{2\pi}{\lambda}$, we obtain that the optimal pitch to achieve fibre-to-waveguide coupling is ([50])

$$\Lambda = \frac{\lambda}{n_{eff} - n_1 \sin\theta}. \tag{2.6}$$

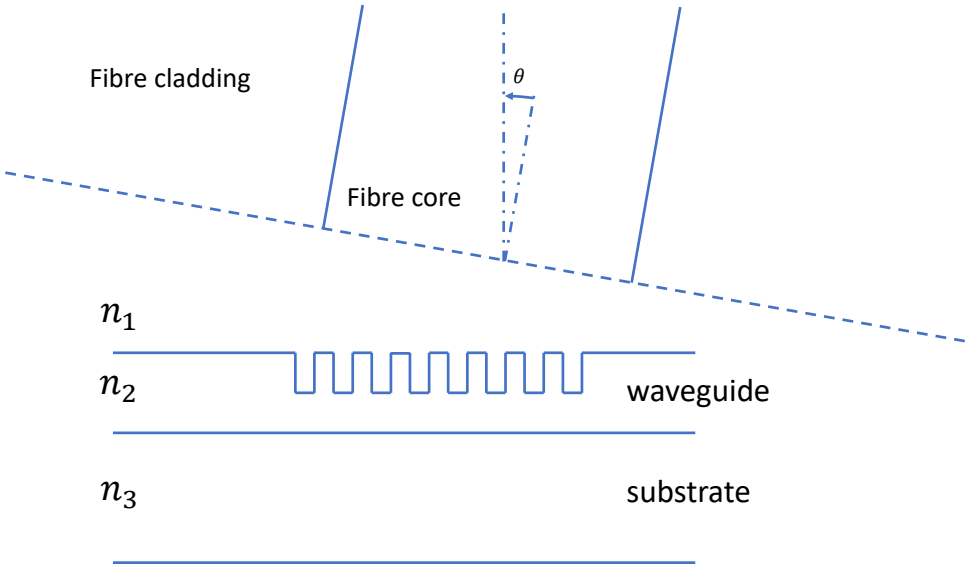

FIGURE 2.4: ***Grating coupler and optical fibre.*** *In this figure we represent the side view of a grating coupler and an optical fibre. In order to couple successfully, constructive interference in the optical field must be achieved. This happen at an angle θ between the fibre and the waveguide.*

2.1.3 Integrated Mach-Zehnder Interfometers

Among the most used components in integrated photonics is the Mach-Zehnder interferometer (MZI). Depending on its specific features, an MZI can be used as tunable beam splitter or as a spectral filter. In general, an MZI is composed of two beam splitters, one in input and one in output, connected by a phase-shifter. In the next two sections I will describe integrated beam-splitters and an integrated phase-shifter.

2.1.3.1 Integrated Couplers: Multimode Interferometer & Directional Coupler

In integrated photonics, there are two main ways to achieve beam splitting operations. The first method is based on *evanescent coupling*, and it is achieved through the use of *directional couplers* (DC) [51]. As shown in Fig. 2.6 DCs consist of two

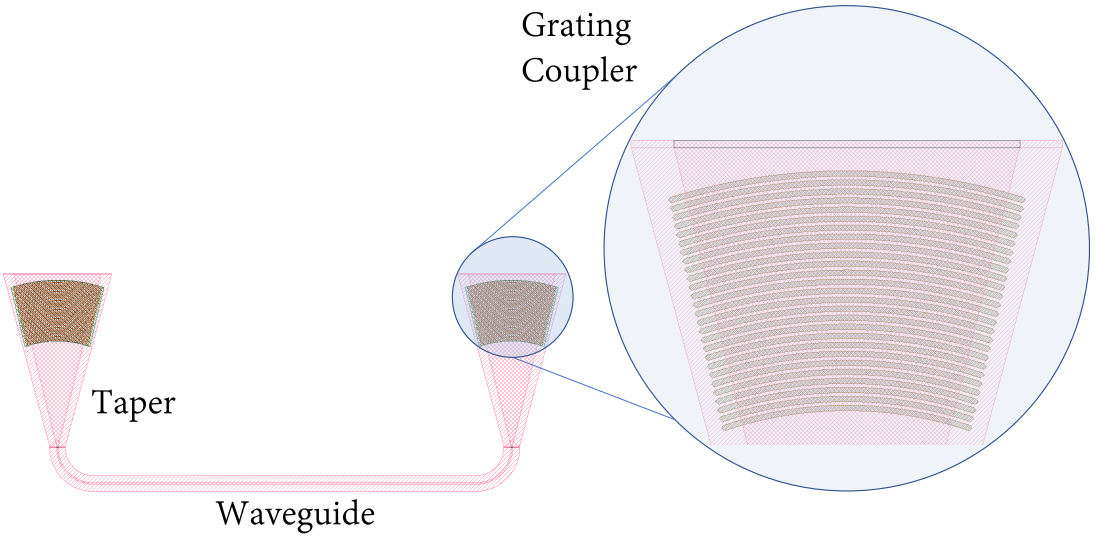

FIGURE 2.5: ***Schematic of grating coupler and a waveguide***. *Here we show a test structure characterised by two grating couplers connected by a waveguide. The grating coupler has a width of a few microns to match the diameter of an optical fibre, and is tapered down to the width of 450 nm, which, for our desing is the width of a single mode waveguide, when working in SOI at 1550 nm. In the zoomed picture, the pattern of the grating coupler can be observed.*

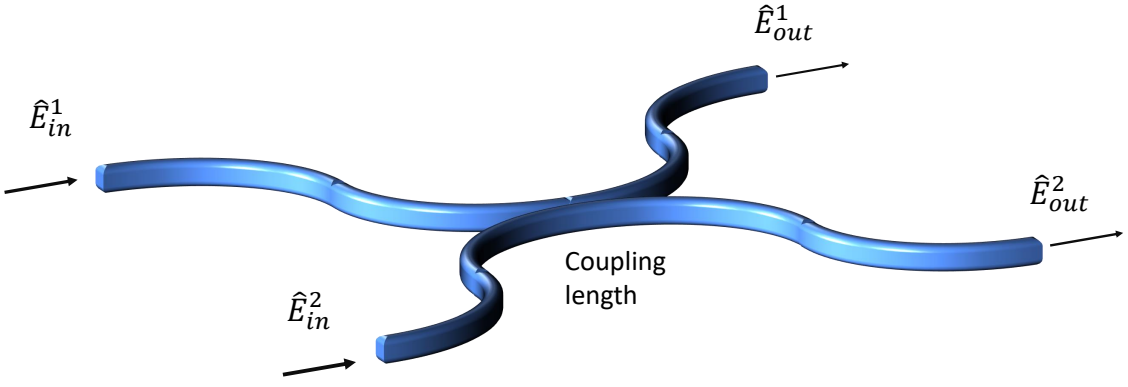

FIGURE 2.6: ***Directional coupler***. *Two single mode waveguides are put close to each other. Depending on the coupling length and the distance between the two waveguides, the desired splitting ratio can be achieved.*

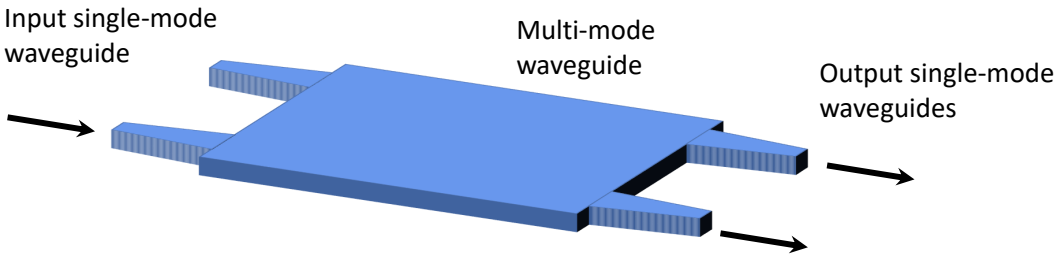

FIGURE 2.7: ***2x2 Multimode Interferometer***. *Two single mode waveguides are injected into a multimode waveguide. At the output of the multimode waveguide, two single mode waveguides are placed. A correct design of the waveguides allows the MMI to work as a 50% integrated beam-splitter.*

single mode waveguides designed in such a way that there is an overlap in the field amplitude in the two waveguides. By properly selecting the shape of the waveguides, the distance between them and the coupling length, the splitting ratio can be tuned. Directional couplers have the advantage of being almost lossless. However, there are a few drawbacks to this approach. First, DC performance are very sensitive on the fabrication process. This has the consequence of making them hardly reproducible. Second, the splitting ratio of DCs strongly depends on the wavelength and this fact drastically reduces the bandwidth of the device.

The second method is based on the *multimode interferometer* (MMI) [52], reported in Fig. 2.7. This interferometer is based on the *self-imaging principle* that, as reported in [52], states: *"Self-imaging is a property of multimode waveguides by which an input field profile is reproduced in single or multiple images at periodic intervals along the propagation direction of the guide."* In this scheme, N single mode waveguides are coupled into a multimode fibre of a given length and width, thus characterised by a given number of allowed modes. This multimode waveguide is coupled back into M single mode waveguides. This particular design allows a certain image to be replicated throughout the multimode waveguide. Therefore, by properly choosing the length of the multimode waveguide, it is possible to couple the modes back into M single mode waveguides. Two examples of self-image are depicted in Fig. 2.8 as reported in [52].

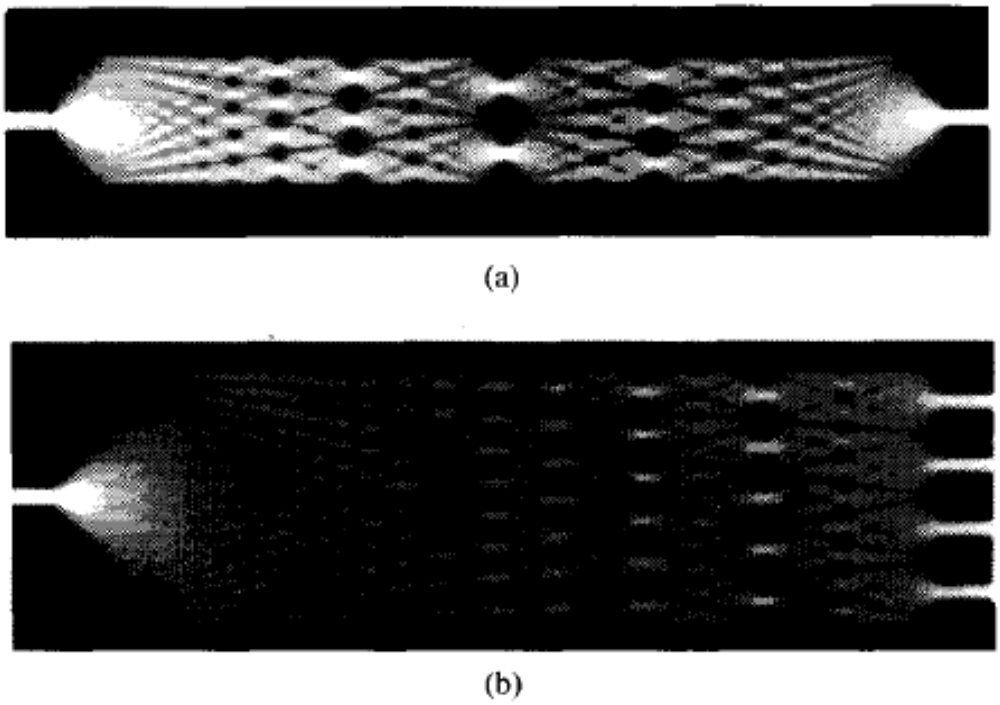

FIGURE 2.8: ***Self-image in a integrated MMI***. *Here the phenomenon of self-imaging is shown from one of the original paper [52].*

2.1.3.2 Integrated Phase modulators: Thermal Phase Shifters

Another fundamental component in optics and integrated optics is the thermal phase shifter (sometimes simply called phase shifter). In integrated photonics, phase modulation can be obtained using different approaches, depending on the properties of the material used. In Silicon, thermal shifters are commonly used. While having a limited maximum speed achievable ($\sim$ 1-10 kHz), thermal shifters provide a low-loss means to control the phase of the optical signals. By changing the temperature of a waveguide by a factor ΔT, the variation in the refractive index

$$\Delta n = \frac{dn}{dT}\Delta T, \tag{2.7}$$

where dn/dT is the thermo-optic coefficient. In silicon the thermo-optic coefficient is ([50])

$$\frac{dn}{dT} = 1.86 \times 10^{-4}/K.$$

The change in phase due to the heating can be thus expressed as

$$\theta = \frac{2\pi L}{\lambda}\Delta n, \tag{2.8}$$

where λ is the wavelength of the light and L is the length of the thermal shifter placed upon the waveguide. Practically, in the Silicon devices used, the thermal shifter consists of a resistive strip of p-doped Silicon grown beside the waveguide and connected to a metal pad on the surface of the chip. The temperature change is achieved by applying a voltage to the metal pad [53].

2.1.3.3 Integrated Mach-Zehnder Interferometer

As previously mentioned, an MZI is composed of two beam-splitters connected by a phase-shifter. In our experiments, we adopted MMIs as integrated beam-splitters. In Fig. 2.9, we represented an MZI based on MMIs and phase modulators.

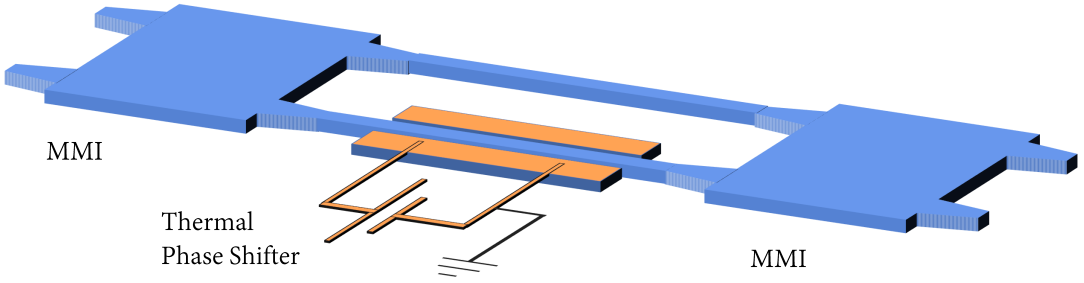

FIGURE 2.9: ***Integrated MZI***. *We report an MZI interferometer integrated in silicon, composed of two MMIs, and an integrated phase modulator.*

2.1.4 Integrated Detectors: photodiodes

In this section we briefly recall the working principle of photodiodes, sketched in Fig. 2.10, and we will describe the main features of photodiodes. In a p-n junction, at the surface between the n-type region and p-type region, a depletion region is created. Thus, an electric field directed from the n-type to the p-type region is generated. When light is injected into the depletion region, electron-hole pairs are created. The holes are attracted in the direction of the electric field and the electrons in the opposite direction. As a result the photocurrent is produced. The main features of a photodiode are the ***Quantum Efficiency*** (or similarly the *Responsivity* $\mathcal{R}$(A/W)), the ***Bandwidth*** and the ***Device Noise***. These features are obtained by making use of a more realistic model of a photodiode, as shown in Fig. 2.11.

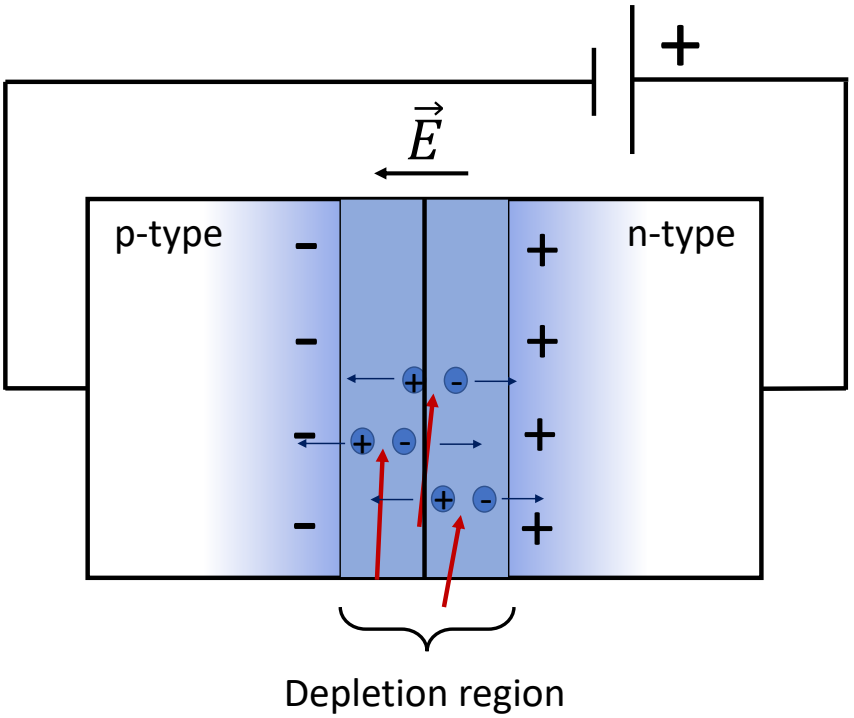

FIGURE 2.10: ***Working principle of a photodiode.*** *A p-n junction can be used as a photodiode. At the edge between the n-type region and the p-type region a depletion region is formed. The light incident in the depletion region creates electron-hole pairs that are directed by the electric field into the same charge region due to the electric field present within the depletion region, so that a current is generated.*

Quantum Efficiency. The quantum efficiency η_{PD} describes the number of electrons produced per incident photon. Therefore it can be written as

$$\eta_{PD} = \frac{n_e}{n_p}, \tag{2.9}$$

where $n_{e(p)}$ is the number of electrons absorbed/photons produced per unit of time. The quantum efficiency is connected to a quantity called *Responsivity*, defined as the ratio between the generated photocurrent and the absorbed optical power

$$\begin{aligned} \mathcal{R} = \frac{I}{P} &= \frac{en_e}{n_p hc}\lambda \\ &= \eta_{PD}\frac{e\lambda}{hc}, \end{aligned} \tag{2.10}$$

where we made use of the $I = en_e$ and $P = n_p hc/\lambda$. At $\lambda = 1550$ nm we obtain

$$\mathcal{R} = 1.25(A/W) \times \eta_{PD}. \tag{2.11}$$

Bandwidth. The bandwidth of a photodiode is the combination of multiple factors: (1) drift time in the depletion region, (2) diffusion of carriers, (3) capacitance of the depletion region. The drift time in the depletion region is due to the width of the depletion region itself and it can minimised by keeping a narrow depletion region. However a not wide enough depletion region increases the capacitance of the junction. This capacitance, combined with the load resistor R_L would act as a low-pass filter, reducing the bandwidth of the device. To reduce the diffusion of carriers, the p-n juction should be built as close as possible to the sensitive surface.

Device Noise. The noise of a photodiode has many sources. The background radiation produces unwanted electron-hole pairs that contribute to the photocurrent. Moreover, pairs are generated by thermal excitation of electrons in the p-n junction. Beside these contributions, there are others related with the electronics used to interface the photodiode to the rest of the system, as for example the load resistor of the photodiode. The noise can be quantified considering the ratio between a given

signal and the noise contribution. A common measure is the NEP ($A/\sqrt{Hz}$) (Noise Equivalent Power).

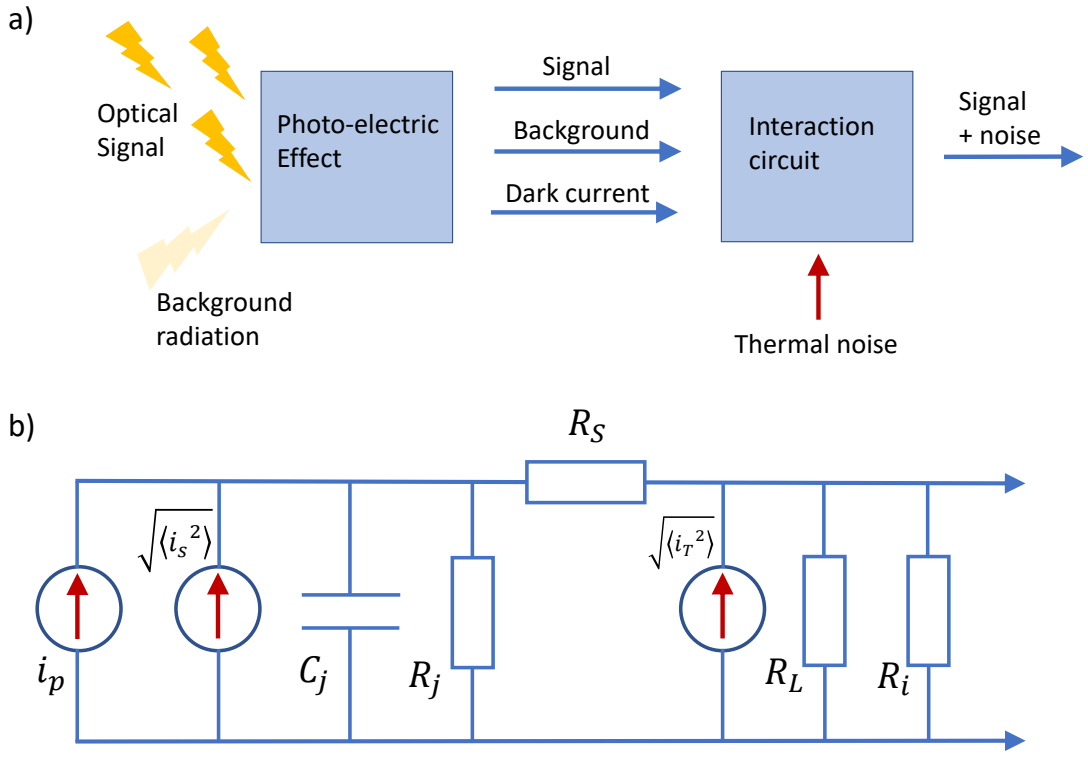

FIGURE 2.11: ***Noise sources of a photodiode.*** *A photodiode has many sources of electrical noise. The background radiation converted into current, as well as the thermally generated electron-hole pairs contribute to the noise. Other contributions come from the electronic components connected to the photodiode (figure from Ref. [54]).*

I-V characteristic curve. The photocurrent emission in relation with the voltage bias applied is described by the *I-V curve*. The photocurrent can be written as

$$I_{PD} = I_0 \left[e^{\frac{qV}{k_B T}} - 1 \right] - I_P, \tag{2.12}$$

where I_{PD} is the photocurrent, I_P is the photocurrent due to the detected optical power, q is the electron charge, V is the voltage applied and k_B and T are respectively the Boltzman constant and the temperature. By looking at Eq. 2.12, we can

observe that for a positive bias the current increases exponentially, independently of the injected light described by I_P. Hence in this situation the photocurrent is just given by dark counts. For V = 0, the photodiode is said to be operated in *photovoltaic mode*. In this case the dark counts are minimised. However, since no electric field is applied to the depletion region, the junction is characterised by higher capacitance due to the small distance between the positive and negative region. Therefore when operating a photodiode in photovoltaic mode, the speed performance are not optimised. For V $<$ 0 the photodiode is said to be operated in *photoconductive mode*. In this case the width of the depletion region is increased, enabling enhanced speed performance, with a partial increase of the dark current. For V $\ll$ 0 the photodiode is said to be in the breakdown voltage region. The reverse voltage applied depends on the specific application and material used. For example, the Ge photodiodes in the SOI platform should be operated with a reverse bias between -1 V and -2 V to optimise the speed performance. Due to a different band gap structure the InP photodiodes should be operated between -5 V and -10 V.

Fabrication Process. The SOI devices used throughout my PhD were fabricated by the IMEC foundry, using the ISIPP25G technology [53, 55]. The photodiodes were fabricated as Si/Ge vertical photodiodes with a p-type contact in the Ge region and a n-type contact in the Si [55]. Given that there is a trade-off between the achievable bandwidth and the efficiency of a photodiode IMEC provides different types of photodiodes, characterised by different speeds and therefore different efficiencies. In our experiments we chose the photodiodes with the highest available efficiency, more revelant in our case than the bandwidth. The main limitation in terms of speed in our experiments is usually the amplification stage, which has bandwidths in general one order of magnitude lower compared to the photodiodes.

The photodetectors in the InP platform where obtained by reverse biasing a 10 μm wide, deep etched semiconductor optical amplifier (SOA) section [56]. The SOA were fabricated via multilayers epitaxial growth processes.

2.1.5 Integrated DBR laser

While the components described in the previous paragraphs are common to the SOI and InP platforms, the great advantage of InP is the possibility of having integrated lasers. The OCLARO foundry that provided our chip described in Chapter 5, provides the integration of DBR lasers. A DBR laser is characterised by a SOA, acting as an active medium, enclosed between two Tunable Bragg Reflectors TBRs, as in Fig. 2.12. As the SOA, the TBRs are fabricated via multilayers epitaxial growth processes and are designed with a top metal layer, to provide electrical connection between the chip and the control electronics. In the SOA region the active layer is obtained as multiple quantum wells. The lasing is achieved by current injection into the SOA. This produces a population inversion which generates the stimulated emission. The TBRs are pin doped waveguide section characterised by periodic corrugations. They can be electrically controlled by current injection to tune the emitted wavelength [56]. The TBR is a pin-doped waveguide region characterised by a periodic corrugation. The peak waveguide can be tuned by injecting current into this region.

2.2 Linear Optics: the Mach-Zehnder Interferometer

In this section we report some results relevant with MZIs. An MZI in general is composed of two beam-splitters, connected through a phase-shifter.

2.2.1 Ideal case

During my Ph.D I have been working with integrated MMIs as beam-splitters. Given that their performance are close to that of an ideal beam-splitter, with a 50:50 splitting ratio and low losses, I will assume ideal beam-splitting operations in the

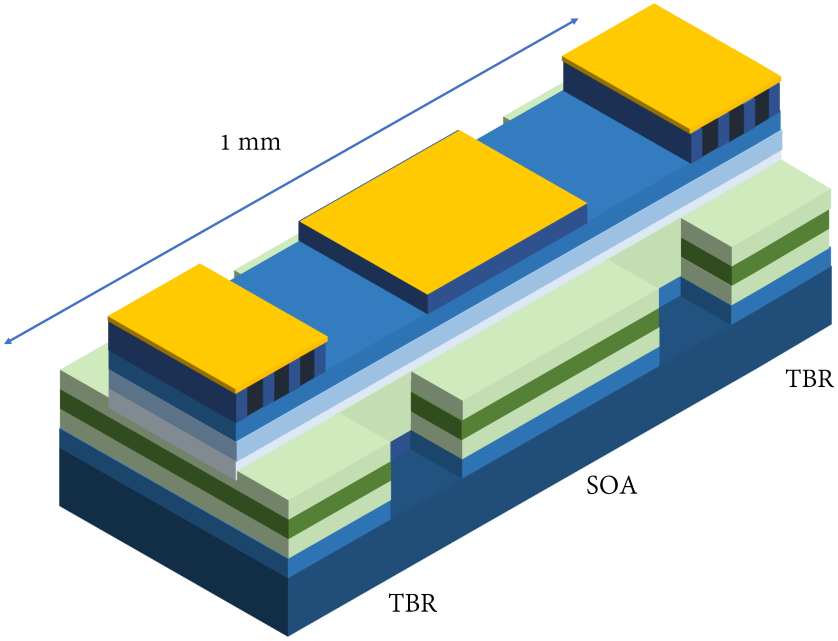

FIGURE 2.12: ***Indium Phosphide integrated DBR laser.*** *In Indium Phosphide a laser can be built by taking advantage of semiconductor optical amplifier (SOA) and two tunable Bragg gratings (TBR). These components can be electrically tuned by connecting the SOA and TBR through the golden plates placed above these components.*

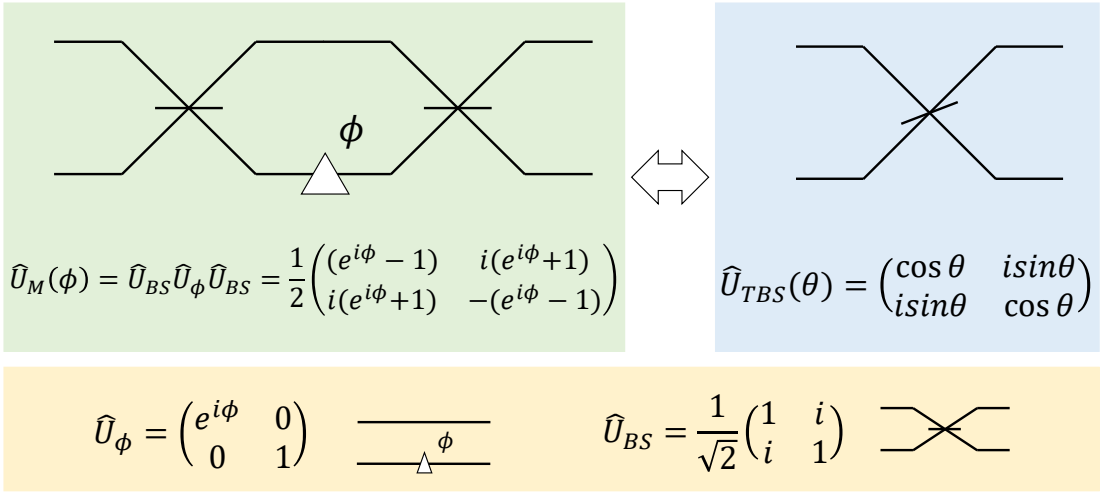

FIGURE 2.13: ***Mapping a tunable MZI into a tunable beam-splitter.*** *We report a pictorial representation of the relation between a tunable MZI and a tunable beam-splitter. This turns to be very useful in our case to correct for any bad splitting ratio in the integrated beam-splitters.*

following. A lossless, balanced MMI can be described by

$$\hat{U}_{BS} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \tag{2.13}$$

while a lossless phase-splitter can be written as

$$\hat{U}_{\phi} = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & 1 \end{pmatrix}, \tag{2.14}$$

where ϕ is the phase difference between the two arms of the phase-shifter. As a consequence, an ideal MZI is described by

$$\hat{U}_M = \frac{1}{2} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} e^{i\phi} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \tag{2.15}$$

$$= \frac{1}{2} \begin{pmatrix} e^{i\phi} - 1 & i(e^{i\phi} + 1) \\ i(e^{i\phi} + 1) & 1 - e^{i\phi} \end{pmatrix}. \tag{2.16}$$

Therefore, considering an input field $E(t) = E_0 e^{-i\omega t}$, injected in the top input (with reference to Fig. 2.13), the intensity at the outputs of the MZI, obtained as the square module of the amplitude field, is for $t = 0$

$$\begin{aligned} I_1 &= \frac{|E_0|^2}{2} (1 + \cos\phi) \\ I_2 &= \frac{|E_0|^2}{2} (1 - \cos\phi) . \end{aligned} \tag{2.17}$$

An important parameter describing the quality of an MZI is the *Visibility*, which is defined (for either I_1 or I_2) as

$$\mathcal{V}_{1(2)} = \frac{I_{1(2)}^{max} - I_{1(2)}^{min}}{I_{1(2)}^{max} + I_{1(2)}^{min}}. \tag{2.18}$$

For an ideal MZI the visibility is $\mathcal{V} = 1$.

It can be noted by Fig. 2.13 that an MZI characterised by a tunable phase-shifter can be mapped onto a beam-splitter with tunable reflectivity. Indeed a lossless beam-splitter with tunable reflectivity can be written as

$$\hat{U}_{TB} = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}. \tag{2.19}$$

This observation suggests that an MZI characterised by tunable beam-splitters can be built as a cascade of phase-shifters and 50:50 beam-splitters, as represented in Fig. 2.13.

2.2.2 Real case: unbalanced interferometer

In Chapter 4 we worked with an integrated unbalanced interferometer. In that case being one arm longer than the other, and given that the linear losses are not negligible, we had to take into consideration this effect when designing and operating the device. While the matrix for the beam-splitter is unchanged from the ideal case, the phase-shifter matrix becomes

$$\hat{U}_{\phi_L} = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & \alpha \end{pmatrix}, \tag{2.20}$$

where $\alpha = e^{-\beta L}$ and β represents the linear losses per unit of length in the longer arm of the phase-shifter. The beam intensity at the output of the unbalanced MZI will become

$$\begin{aligned} I_1^{loss} &= \frac{|E_0|^2}{4}\left(1+\alpha^2+2\alpha\cos\phi\right) \\ I_2^{loss} &= \frac{|E_0|^2}{4}\left(1+\alpha^2-2\alpha\cos\phi\right). \end{aligned} \tag{2.21}$$

The visibility in this case becomes

$$\mathcal{V}_{1(2)}^{loss} = \frac{2\alpha}{1+\alpha^2}. \tag{2.22}$$

Therefore the visibility of an unbalanced MZI is reduced by the amount of imbalance. For example, for $\alpha = 0.5$ the visibility is reduced to $\mathcal{V}_{1(2)}^{loss} = 0.8$. On the other hand,

we observe that the condition $\alpha = 1$ corresponds to the previous situation of a lossless phase-shifter.

2.2.3 Tunable MZI

Linear losses are among the main limitations when working in Silicon photonics. This is particularly true when dealing with delay lines, given that, for example, the losses in our devices were estimated to be $\alpha \sim -2$ dB/cm in the strip waveguides and $\alpha \sim$ -1 dB/cm in the rib waveguides used in the delay line. In the case of unbalanced MZIs, linear losses have the main effect of reducing the visibility and the optical power at the output of the MZI itself. A partial solution to this problem is a tunable MZI, i.e. an MZI with tunable beam-splitters. This is achieved, as previously mentioned, by using a MZI where the input and output beam-splitters are two tunable MZIs. Following from Fig. 2.13, in Fig. 2.14 we report the scheme of a tunable MZI. A tunable MZI is therefore described by

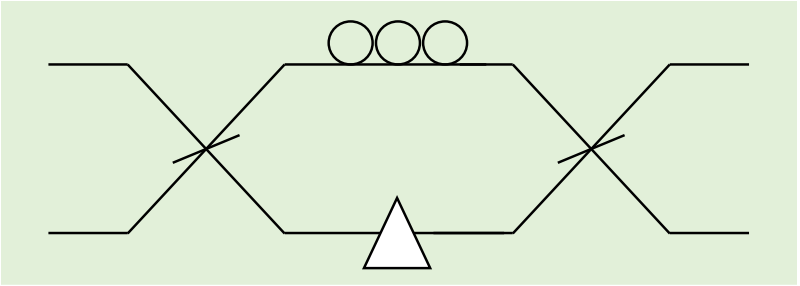

FIGURE 2.14: ***Tunable MZI.*** *Scheme of a tunable MZI composed of a two tunable beam-splitters and a phase shifter characterised by a lossy delay line.*

$$\begin{aligned} \hat{U}_{TM} &= \hat{U}_{TB}\hat{U}_{\phi_L}\hat{U}_{TB} \\ &= \begin{pmatrix} \cos\theta_2 & i\sin\theta_2 \\ i\sin\theta_2 & \cos\theta_2 \end{pmatrix} \begin{pmatrix} e^{i\phi} & 0 \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} \cos\theta_1 & i\sin\theta_1 \\ i\sin\theta_1 & \cos\theta_1 \end{pmatrix}. \end{aligned} \tag{2.23}$$

Therefore, for a field $E(t) = E_0 e^{i\omega t}$ injected on the top arm of the tunable MZI, we get

$$I_1 = |E_0|^2 \left[1 - \sin^2\theta_1 - \sin^2\theta_2 + \left(1+\alpha^2\right)\sin^2\theta_1 \sin^2\theta_2 - f_\alpha \cos\phi\right] \quad (2.24)$$

$$I_2 = |E_0|^2 \left[\left(1 - \sin^2\theta_1\right)\sin^2\theta_2 + \alpha^2\left(1 - \sin^2\theta_2\right)\sin^2\theta_1 + f_\alpha \cos\phi\right], \quad (2.25)$$

where $f_\alpha = 2\alpha \cos\theta_1 \cos\theta_2 \sin\theta_1 \sin\theta_2$. Finally, for a tunable Mach-Zehnder interferometer based on tunable, lossless beam-splitters and a lossy phase-shifter, the visibility becomes

$$\mathcal{V}^1_{tun} = \frac{f_\alpha}{1 + (\alpha^2+1)\sin^2\theta_1 \sin^2\theta_2 - \sin^2\theta_1 - \sin^2\theta_2} \quad (2.26)$$

$$\mathcal{V}^2_{tun} = \frac{f_\alpha}{(1 - \sin^2\theta_1)\sin^2\theta_2 + \alpha^2(1 - \sin^2\theta_2)\sin^2\theta_1} \quad (2.27)$$

It can be observed that, depending on the value of α, by adjusting the reflectivity of the tunable beam-splitters it is possible to maximise the visibility.

2.3 Phase-space description & Wigner Function

In Chapter 3, beside the demonstration of an integrated quantum random number generator, we showed that our homodyne detector has the features to properly reconstruct quantum states of light. Here we will give a brief description of the *Wigner quasi-probability distribution* (or briefly Wigner function), which provides a complete description of quantum states in the phase-space. The concept of Wigner function was developed to provide a tool to describe quantum states in the phase-space, similar to what happens in classical mechanics or classical electromagnetism. A good intuitive description was introduced in [57] and reported also in [58]. In classical mechanics, the state of a system can be described by the knowledge of q and p in the phase-space, or by the distribution $W_{class}(q,p)$. The same formalism can be used to describe classical electromagnetic fields by means of the complex amplitude α. The complete knowledge of q and p, or otherwise the knowledge of α in the

case of EM fields, provides a full description of the system considered. In quantum mechanics things change drastically, given that the *Heisenberg Principle* prevents us from gathering complete simultaneous information about q and p at the same time. Moreover, in quantum mechanics we cannot even measure the state of a system with certainty because when we measure a physical system prepared in a particular state the outcome is probabilistic. The intuition behind the Wigner quasi-probability $W(q,p)$ distribution was therefore as follows: the Wigner function should be a joint distribution of the quadratures q and p, such that the outcome of a measurement on either q or p, should yield the expected probability distribution (usually called *marginal distribution*). In other words $\int W(q,p)dp$ and $\int W(q,p)dq$ should yield the correct distributions for q and p. Additionally, a shift by a phase θ in the quadratures should give a rotated probability distribution, similar to what happens in classical physics. Here also lies the strong connection between the intuition of the Wigner quasi-probability distribution, and homodyne detection measurements, described by Eq. 2.36 in Section 2.3.2.

2.3.1 Examples of Wigner function

Formally, the Wigner function $W(q,p)$ is defined as [58]

$$W(q,p) = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{ipx}\Big\langle q - \frac{x}{2}\Big|\hat{\rho}\Big|q + \frac{x}{2}\Big\rangle dx. \tag{2.28}$$

where the density matrix is $\hat{\rho} = |\psi\rangle\langle\psi|$.

The simplest case of Wigner function is that of vacuum states. From Eqs. 2.28 and 2.45, given that $\psi(x) \equiv \langle x|\psi\rangle$, we have

$$W_0(q,p) = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{ipx}\psi^*\left(q + \frac{x}{2}\right)\psi\left(q - \frac{x}{2}\right)dx. \tag{2.29}$$

By solving the previous integral we get

$$W_0(q,p) = \frac{1}{\pi}\exp\Big(-q^2 - p^2\Big). \tag{2.30}$$

We observe that the vacuum states are described as Gaussian distributions centered in $(q = 0, p = 0)$, with variance equal to 1/2. Similarly, coherent states are described by displaced Gaussian distributions, such that

$$W_\alpha(q,p) = \frac{1}{\pi}\exp\{-\left[(q-q_0)^2 + (p-p_0)^2\right]\}, \tag{2.31}$$

where q_0 and p_0 are the projections of α along the q and p axis, i.e. $\alpha = q_0 + ip_0$.

2.3.2 Measuring the Wigner Function: Homodyne Detection

Homodyne detection is a technique used to measure quantum states, by determining their Wigner quasi-distribution and density matrix [22]. A weak quantum optical signal $\hat{E}_S$ is interfered at a beam splitter with a strong coherent beam called local oscillator (LO), described by $\hat{E}_{LO}$. This is shown in Fig. 2.15. The outputs can be written as

$$\begin{aligned} \hat{E}_1 &= \frac{1}{\sqrt{2}}(\hat{E}_S + i\hat{E}_{LO}) \\ \hat{E}_2 &= \frac{i}{\sqrt{2}}(\hat{E}_S - i\hat{E}_{LO}). \end{aligned} \tag{2.32}$$

The optical intensities detected at the photodiodes can be written as

$$\begin{aligned} \hat{I}_1 &= |\hat{E}_1|^2 = \frac{1}{2}(\hat{E}_S^\dagger - i\hat{E}_{LO}^\dagger)(\hat{E}_S + i\hat{E}_{LO}) \\ \hat{I}_2 &= |\hat{E}_2|^2 = \frac{1}{2}(\hat{E}_S^\dagger + i\hat{E}_{LO}^\dagger)(\hat{E}_S - i\hat{E}_{LO}). \end{aligned} \tag{2.33}$$

The LO is a strong coherent beam and thus it can be written as $\hat{E}_{LO}^+ = |\alpha|e^{i\theta_L}$. On the other hand, the quantum signal is $\hat{E} = \hat{a}^\dagger e^{i\theta_S} + \hat{a}e^{-i\theta_S}$. As a consequence, the subtracted photocurrent will be

$$\hat{I}_- \equiv \hat{I}_1 - \hat{I}_2 = 2i|\alpha|\left(\hat{a}^\dagger e^{i\theta} - \hat{a}e^{-i\theta}\right) \propto |\alpha|\hat{q}(\theta) \tag{2.34}$$

Therefore, the subtracted intensity is proportional to the quadrature of the quantum signal $\hat{E}_S$, where θ is the relative phase between signal and LO. Hence, suppose that

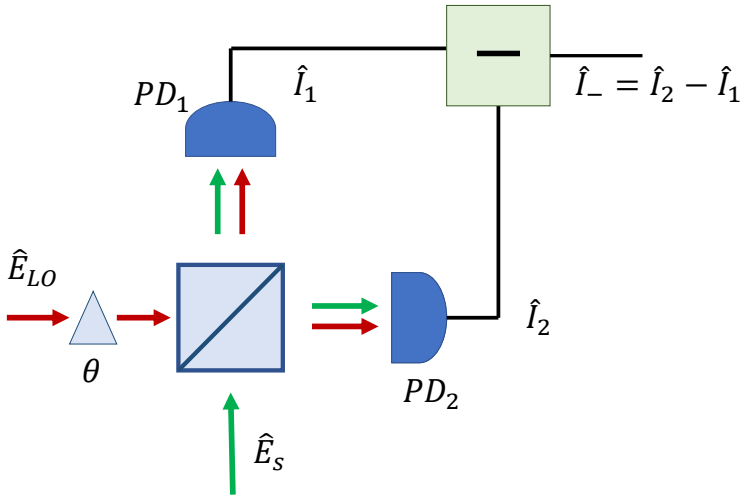

FIGURE 2.15: ***Scheme of a homodyne detection.*** *Here we report a simplified scheme of a homodyne detector. An optical quantum signal $\hat{E}_S$ is interfered at a balanced beam-splitter with a strong coherent beam described by $\hat{E}_{LO}$. The outputs are detected by two photodiodes, and the resulting photocurrent are subtracted by some electronic device.*

a quantum state is described by a density matrix $\hat{\rho}$, the probability of measuring a value for the quadrature equal to q_θ is

$$Pr(q_\theta, \theta) = \langle q_\theta, \theta | \hat{\rho} | q_\theta, \theta \rangle, \tag{2.35}$$

where $|q_\theta, \theta\rangle$ is the quadrature eigenstate with eigenvalue q_θ.

The probability $Pr(q_\theta, \theta)$ is called *marginal distribution* and it is the quantity that is experimentally measured with a homodyne detector. This quantity is directly connected to the Wigner function. As shown in Fig. 2.16, the marginal distribution is the projection of the Wigner function on a vertical plane at an angle θ in the phase-space

$$Pr(q_\theta, \theta) = \int_{-\infty}^{+\infty} W(q_\theta \cos\theta - p_\theta \sin\theta, q_\theta \sin\theta + p_\theta \cos\theta) dp_\theta. \tag{2.36}$$

In order to reconstruct a quantum state, a set of marginal distributions must be acquired at different angles, i.e. at different phases of the LO. The actual reconstruction of $W(q,p)$ would require the inversion of Eq. 2.36, as performed in [59] to reconstruct the Wigner function of a single photon. An iterative algorihtm that avoids the inversion of Eq. 2.36 was envisaged in [60] and it has been widely used in the last few years.

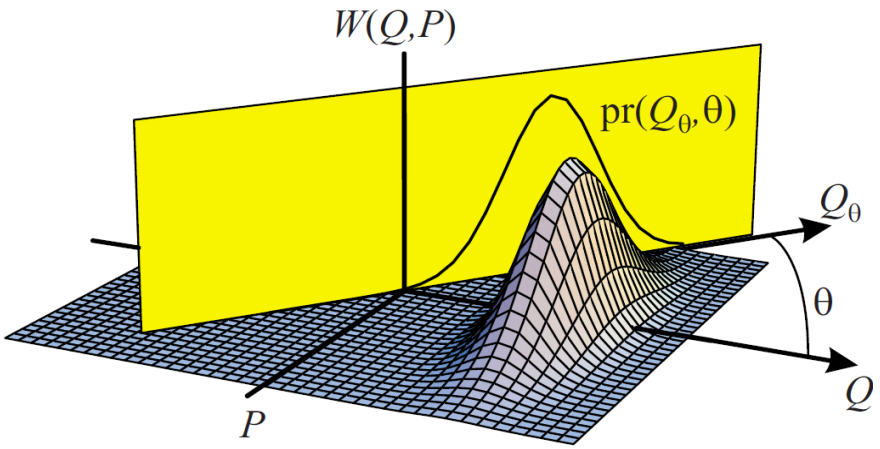

FIGURE 2.16: ***Representation of a Wigner function and the marginal distribution.*** *We report a 3D representation of the Wigner function and the marginal distribution, obtained by projecting the Wigner function on a vertical plane defined by the phase θ (in the picture the yellow plane), as reported in [22].*

2.4 Quantum Random Number Generators

2.4.1 Probabilistic Nature of Quantum-Mechanics

In the textbook *Quantum Mechanics* (Konishi and Paffuti [61]), it is stated that

"the fundamental postulate of quantum mechanics asserts that the probability of findind a result f_n in the measurement of a quantity f made in the state $|\psi\rangle = \sum_n c_n \psi_n(q)$ is given by

$$P_n = |c_n|^2."$$

This postulate is completed by another postulate which states that

"the system immediately after the measurement that gave a result f_n, is in the state $|\psi\rangle = |n\rangle$ where the projector $\mathcal{P}_n \equiv |n\rangle\langle n|$."

These postulates express the probabilistic nature of Quantum Mechanics and they have been the theoretical foundation for the development of QRNGs. Most of the recent demonstrations of QRNGs are based on optical systems [1] and two main approaches have been developed, based either on discrete or continuous variable.

2.4.1.1 Randomness in Discrete Variable

In the discrete-variable framework, a QRNG was first proposed at the end of the 20th century [15, 16]. A simple example of QRNG based on discrete-variable, can be that of a single photon, entering a 50:50 beam-splitter, as depicted in Fig. 2.17. The overall system at the outputs of the beam-splitter can be written as

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \tag{2.37}$$

where $|0\rangle$ and $|1\rangle$ label respectively the vertical and horizontal path at the beam-splitter's outputs. Therefore, the probability of observing a photon at the detector $D_{0/1}$ will be

$$P_0 = |\langle 0|\psi\rangle|^2 = \frac{1}{2} \tag{2.38}$$

$$P_1 = |\langle 1|\psi\rangle|^2 = \frac{1}{2}. \tag{2.39}$$

As a consequence, by labelling respectively with 0 and 1 the single photon measurements at the detectors D_0 and D_1, it is possible to obtain a perfectly unbiased string of 0s and 1s.

QRNG based on qubit encoded in different degrees of freedom have been demonstrated, such as time-bin, polarisation and path encoding (see [1] for a recent review

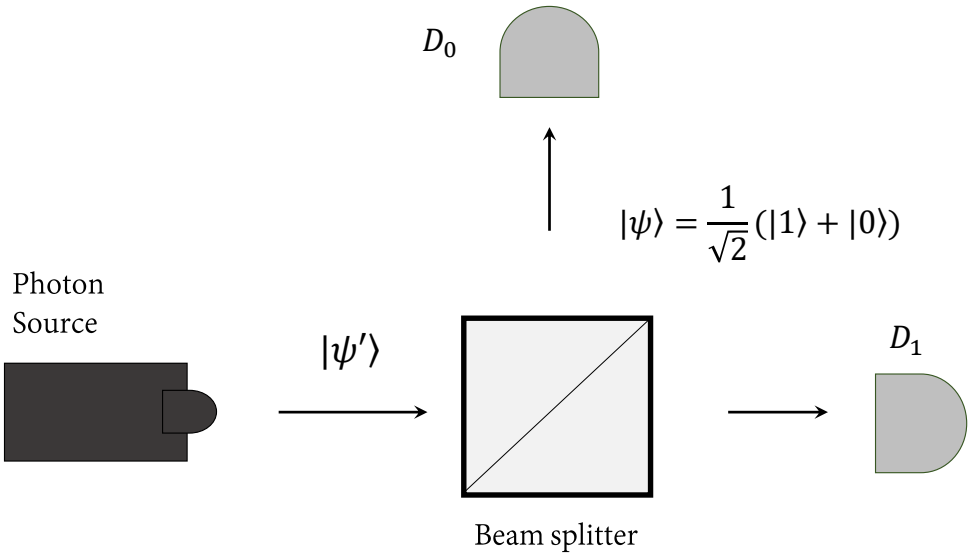

FIGURE 2.17: **Discrete variable QRNG**. *A single photon enters a* $50:50$ *beam spitter. The state in output is in a superposition of the two possible outputs. Since the projection either the two eigenstates is probabilistic, by recording a sequence of subsequent measurements it will be possible to obtain a string of random, unpredictable bits.*

and the Introduction chapter). A very interesting aspect is the level of characterization of the device required, which depend on the degree of control that a potential adversary might possess on the device [62]. For QRNGs different levels of security can be assumed based on the hacking power of a potential eavesdropper. This can range from a *tomography level* where it is assumed that the adversary does not have any power to affect the system, (but they might have perfect knowledge of the device) to *device independent* where the adversary can be the provider of the system itself. In the first case, in order to avoid the leakage of information, the device must be characterized in all the relevant degrees of freedom. Unchecked parameters could be used by an eavesdropper to extract information about the input states and about the measurements. In the second case the security does not rely on the features of the device but simply on the statistics of the measurements. This must be done by taking advantage of Bell's inequality measurements [13, 14]. An example of random numbers certified by the Bell's inequality was performed back in 2010 not by means

of optical systems, but by entangling two atoms [63]. This particular scheme allowed them to violate the Bell's inequality with almost perfect efficiency, although with incredibly low generation rates. More recently there have been a few demonstrations of optical QRNGs based on Bell's inequality violation [64]. This particular kind of device-independent QRNG was indeed performed in the discrete-variable framework, which in this particular aspect is superior to the continuous-variable counterpart.

2.4.1.2 Randomness in Continuous Variables

While the discrete-variable picture is quite intuitive, in the continuous-variable picture, the situation is slightly more complicated. Once more however, the randomness derives from the probabilistic interpretation of measurements in Quantum Mechanics. Here we consider optical vacuum states in the phase-space. Coherent states are eigenvalues of the annihilation operator $\hat{a}$, and hence we can write

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle, \tag{2.40}$$

where, in the Fock space $|\alpha\rangle$ can be expressed as

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{(\alpha^n a^\dagger)^n}{n!}|0\rangle. \tag{2.41}$$

In the phase-space, the relation between the annihilation and creator operators $\hat{a}$ and $\hat{a}^\dagger$ with the quadratures $\hat{q}$ and $\hat{p}$ is

$$\begin{aligned} \hat{a}^\dagger &= \frac{1}{\sqrt{2}}(\hat{q} - i\hat{p}) = \frac{1}{\sqrt{2}}(q - \frac{d}{dq}) \\ \hat{a} &= \frac{1}{\sqrt{2}}(\hat{q} + i\hat{p}) = \frac{1}{\sqrt{2}}(q + \frac{d}{dq}) \end{aligned} \tag{2.42}$$

and therefore Eq. 2.40 can be written as

$$\frac{1}{\sqrt{2}}\left(q + \frac{d}{dq}\right)\psi(q) = \alpha\psi(q), \tag{2.43}$$

which for $\alpha = 0$ becomes

$$\left(q + \frac{d}{dq}\right)\psi(q) = 0. \tag{2.44}$$

By solving Eq. 2.44, we obtain the wavefuction for the vacuum state as

$$\psi_0(q) = \frac{1}{\pi^{1/4}} \exp\left[-\frac{q^2}{2}\right]. \tag{2.45}$$

Hence, given that $\langle q|\psi\rangle \equiv \psi(q)$ the probability of measuring a particular value q, when measuring the quadrature $\hat{Q}$, for a vacuum state is

$$Pr_0(q) = |\psi_0(q)|^2 = \frac{1}{\pi^{1/2}} \exp\left[-q^2\right]. \tag{2.46}$$

Therefore, while in the discrete-variable picture the probability assumes discrete values, in the continuous-variable paradigm the probability is described by a continuous distribution. In particular, for optical vacuum states we have a Gaussian distribution with a variance equal to 1/2. Finally, as in the case of single photons injected into a 50:50 beam-splitter, by measuring optical vacuum states, it is possible to generate sequences or random bits. Indeed, each single measurement is unpredictable and normally distributed.

In Chapter 4 a QRNG based on phase fluctuations from a laser diode is reported. Although usually with the term continuous-variable we refer to the Quantum Optics described in the phase-space, throughout this thesis I will refer to the phase fluctuation approach also as continuous-variable, implying that neither single photon generation nor single photon detection are involved.

2.4.2 General Protocol of a QRNG

In the last few years many QRNGs have been demonstrated, both in discrete and continuous-variable. Despite different schemes being used, the overall protocols to

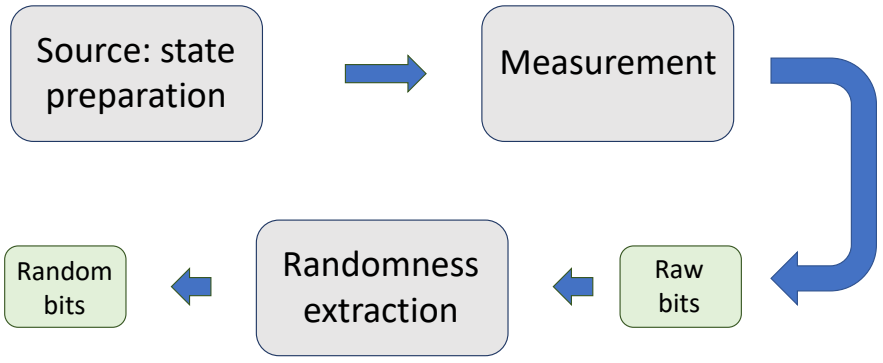

FIGURE 2.18: ***General QRNG protocol description.*** *Here we show how a general optical QRNG works. An optical source prepares the states (coherent, squeezed, single photons etc.) that are measured by some detection scheme (photodiodes, single photon detectors). After the measurement, the raw bits are extracted, and often a randomness extractor is used to eliminate the bias due to the imperfections in the system.*

generate random numbers can be described as a sequence of a few common building blocks [65] (see Fig. 2.18).

- **Source and state preparation:** In optical QRNG the primary source can be either a laser, a LED or any other light source. Moreover, depending on the specific scheme used, the light source can be followed by some device to manipulate the light, for example, to produce Fock states, entangled states or strongly attenuated coherent beams. Therefore, there will be QRNGs with a very simple source device (i.e. coherent or thermal light) and others characterised by a more complex source device, particularly when entangled states or single photons are involved.

- **Measurement Device:** Similar to the source device, the complexity of the measurement device will depend on the specific scheme. In the discrete-variable description, single photon detectors are used – this has a few consequences such as the requirement for cryogenic temperatures, necessary to reach high detection efficiency and to minimise dark counts [66]. Moreover, single photon detectors have a maximum operation rate in the MHz regime,

which could limit the final generation rate of the QRNG. On the other hand, in the continuous variable schemes, photodiodes are often used to detect light. High efficiency photodiodes can reach bandwidth of a few tens of GHz, potentially lifting the generation rates of many orders of magnitude, without the need of cryogenic temperatures, making their use more practical.

- **Randomness Extraction:** Depending on the quality of the raw random bits generated as outcomes of the measurements, another step of randomness extraction is necessary, this is because the imperfections in the experimental devices can bias the random bits as well as the different forms of environmental noise.

As explained in the Introduction, different approaches have been used, based either on discrete-variable or continuous-variable schemes.

In the following Chapters we will describe three different QRNGs based on continuous-variable quantum optics. These schemes take advantage of laser sources, linear optics and photodiodes to detect the output light. While the source and measurement devices of our experiments will be explained in each result chapter, here we will give briefly background information regarding the randomness extraction stage, which is common to Chapter 3 and 4.

2.4.2.1 Min-entropy as a Measure of Randomness

One of the main building blocks of a QRNG is the randomness extractor. Even though the source and measurement device used to produce random numbers can be shown to be *quantum* by some model that takes advantage of the laws of Quantum Mechanics, the practical realisation of both source and measurement possesses some *classical noise* mixed up with the quantum signal. This classical noise, whatever might be its origin, can introduce biases in the random sequences. Examples of noise could be environmental noise, such as RF frequency or any noise introduced by the electronic instruments used. Another source of bias could be the actual

distribution of the signal, as in Chapters 3 and 4, where the random bits were extracted by Gaussian distributions, where some bit sequences were more likely to appear. Therefore a randomness extraction step was required to obtain a final unbiased sequence of random bits. The first step in the randomness extraction consisted in quantifying the randomness present in the output. Throughout my thesis I made use of the *min-entropy* to quantify the raw randomness produced.

The min-entropy $H_\infty(X)$ is defined as

$$\mathrm{H}_\infty = -\log_2(\max_{x\in\mathcal{A}}\Pr[X=x]), \tag{2.47}$$

where X is a distribution and x a possible outcome belonging to a set $\mathcal{A}$. It describes the probability of guessing, at the first attempt, the outcome from a known distribution. Hence, for a known distribution with min-entropy $H_\infty = k$, the probability of guessing a specific outcome is

$$P_{guess} = 2^{-k}. \tag{2.48}$$

One of the great advantages of the min-entropy is that it can be interpreted as the number of uniform bits that can be extracted from a given distribution [67, 68], and as shown in [65], it can be used to perform theoretically proven randomness extraction.

It is important here to recall that Eq. 2.47 is valid only when a few assumptions on the signal are satisfied [65]:

- The quantum and classical signals are independent. This means that while the classical noise can affect the overall raw signal, once the classical noise has been characterised and quantified, the quantum noise is considered having the expected distribution.
- The total variance σ^2 can be determined by sampling the raw signal. This implies that the samples are independent and identically distributed (iid). In practise we assume that the residual classical noise, being small compared to

the quantum signal, do not affect the entropy estimation. This can be verified by measuring the power spectral density of the signal compared to the power spectral density of the background electronic noise. As a counterexample, the bit string 01010101010101 is characterised by a uniform distribution, where the number of 1s equals the number of 0s. The calculated min-entropy would be $H_\infty = 1$ and hence the maximum achievable for 1 bit samples. However, this sequence is perfectly anti-correlated and therefore highly predictable.

- $\Pr[X = x]$ being the distribution of the quantum signal is known or can be determined. Otherwise it is not possible to distinguish the quantum signal from the classical noise, that is always present in real-world processes. In our case this assumption is satisfied being the quantum and classical signals characterised by Gaussian distributions.

2.4.2.2 Toeplitz Extractor

In terms of randomness extraction, many solutions have been used in the past such as the bit-wise XOR operation between subsequent bits [32] or the Least-significant-bit (LSB) method [69]. While these methods are rather efficient when implemented both via software or via hardware and while they provide good randomization of the raw data, they are not information-theoretically provable, which means that no theoretical demonstration can be used to prove their security. For this reason in our experiments we followed the post-processing method proposed in [65], using as a randomness extractor the Toeplitz algorithm. The Toeplitz extractor has a few relevant properties that make it an ideal solution in QRNG. First, it is a universal hashing, which means that the probability that the application of the same matrix on different vectors gives the same outcome is close to zero. As a consequence, the Toeplitz extractor is a strong extractor, that is, it can be reused without the need of a new matrix for each new raw bit-string. Second, the Toeplitz algorithm, being based on a bit-wise matrix multiplication, can be implemented via hardware, for example through high-speed FPGA [70]. The working principle of the Toeplitz

extractor is the following: from a raw bit string of a given length n, obtained as a result of the measurement, the estimated min-entropy of the quantum signal is extracted by taking advantage of the assumptions made on that specific QRNG. For $H_\infty = k$, a string of $m = n \times k$ bits is used to built a $m \times n$ Toeplitz matrix[1]. The hashed sequence will be obtained by multiplying the raw string by the Toeplitz matrix. The result of this operation will be a bit-string characterized by a uniform distribution. While it is not obvious at first sight how a Gaussian-distributed bit-string is mapped into a uniform bit-string, an indication could be given by how a vector-matrix multiplication works. In a vector-matrix multiplication each line of the matrix is multiplied by the vector, element by element. Given that the Toeplitz matrix is composed by a first row (and column) of random bits, and given that a bit-wise sum operation is performed between the bit of the matrix and those of the raw bit-string, the first bit of the resulting bit-string will be random. This is because a single random bit in the whole first row would be sufficient to yield a random bit as an outcome (and the whole first row of the matrix is random). Because of the construction of the Toeplitz matrix, the same argument is valid for each row. While the matrix is diagonally repeated, each line starts with a random bit, that will affect the final result. Moreover, the size of a Toeplitz matrix is usually beyond 1000×1000, therefore it can be understood that the residual correlations and biases are lost after the multiplication of the vector of raw bits by a large Toeplitz matrix. It can be noted that to build a random $m \times n$ Toeplitz matrix, $m + n - 1$ random bits are needed. Therefore if a new set of random bits were needed for each sequence, no randomness could be generated. However, as mentioned above, the Toeplitz method is a strong extractor. This has the implication that the same seed can be reused without compromising the randomness of the output sequence [65]. It is worth noting that other information-theoretically provable strong extractors exist, for example the Trevisan extractor, which has the advantage of requiring fewer bits than the Toeplitz and being secure against quantum adversaries [65]. However the main advantage of the Toeplitz algorithm is that it is faster, when performed via

[1]The Toeplitz matrix is obtained by diagonally repeating the first row and column (see Fig. 2.19).

software, than the Trevisan extractor. Moreover the Toeplitz extractor, as opposed to the Trevisan extractor, can be performed in FPGA, providing a great advantage in terms of final generation rates.

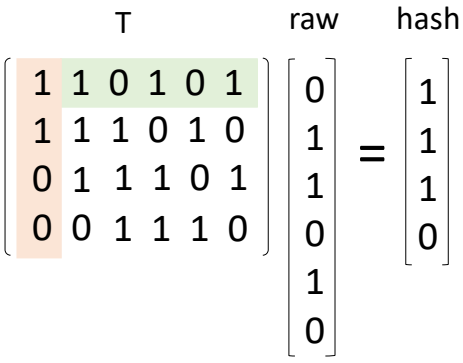

FIGURE 2.19: ***Toeplitz matrix multiplication***. *T is Toeplitz matrix obtained by copying the elements from the first row and first column diagonally. It is multiplied by a vector of raw random data in a bit-wise sum operation. The result is the vector of hashed data.*

2.4.3 Randomness testing

In order to certify the quality of our QRNGs, we used a set of 15 different statistical tests provided by the National Institute of Standards and Technology (NIST SP 800-22) [71]. This battery of tests looks for different possible patterns among the bits that would reduce the randomness of the data generated. Each test is based on the P-value, so we will also give a brief description of the statistical hypothesis testing using P-value.

2.4.3.1 NIST statistical tests suite

The NIST statistical tests suite is composed of 15 tests that check different features of the random number generator. A description for each test can be found in [71]. As previously mentioned, these tests are based on the P-value method. For each test the suite works as follows:

- a file of random bits is split into a number of blocks of a given length (usually more than one million bits).
- for each block the statistical test is applied and a P-value is extracted. If the P-value is above a minimum value (usually > 0.01) then the single test is *passed*.
- For each test, the P-values from the different blocks are collected and the distribution of P-values is calculated.
- A second test of P-value is applied to this distribution, where the null-hypothesis verifies if the P-values coming from all the different blocks are uniformly distributed[2].
- These are the P-values that are shown in the final table of the results for the statistical tests. In order for a test to be passed this has to be above 0.01.
- In the final table usually the proportion of blocks that passed the tests is reported, and a minimum number of blocks must pass the test in order for the block to be considered random.

2.4.3.2 P-value

In statistical hypothesis testing, the P-value, represented in Fig. 2.20, describes [73]

"the probability of getting the same or more extreme results than those observed, under the assumption that some null-hypothesis, usually referred as H_0, is verified.".

In the context of generation of random bits through quantum processes, the P-value can be phrased as follows:

[2]The uniformity of P-values implies that the null hypothesis is verified [72].

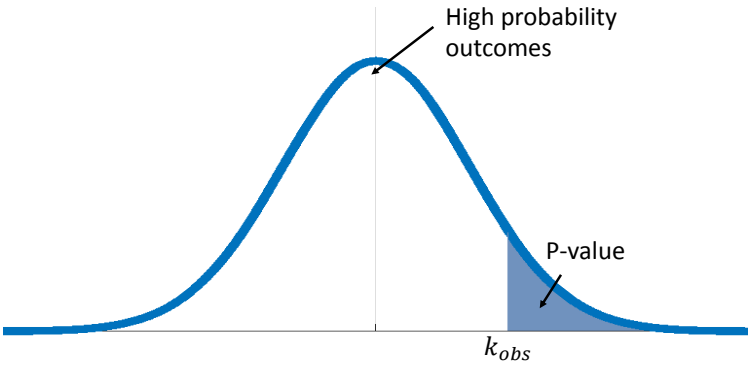

FIGURE 2.20: ***Example on statistical Hypothesis testing: P-value.*** *We report a pictorial representation of statistical hypothesis testing, using the P-value. Here is represented the distribution of the possible outcomes, with the relative probabilities. The shadowed area describes the area such that $k > k_{obs}$ and thus, it corresponds to the probability of obtaining more extreme data than the ones observed, given that specific null-hypothesis. The shadowed area is the P-value.*

"the probability of getting more biased results than those observed, under the assumption that these bits were generated by a perfect quantum random numbers generator.".

In these definitions, the word *biased* and the null-hypothesis H_0 depend on the statistical test applied to the random numbers. For example, if the test is checking whether the number of 1s and 0s is consistent with a fair generator, the null-hypothesis will be that we expect the same number of 0s and 1s and the word *biased* will be referring to the situation where the number of 0s (or 1s) is much greater than the number of 1s (0s). An important characteristic of P-values is that, under the null-hypothesis, the P-values obtained after the repetition of an experiment should be uniformly distributed.

Here we recall that the results of the application of the NIST test on a QRNG does not give any information about the *quantumness* of the generator. The quantumness in our case was characterised at the preliminary stage of each experiment and the procedure was depending on the physical realisation of the QRNG.

Chapter 3

A homodyne detector integrated into an SOI chip to measure coherent states and generate random numbers

This chapter is based on the results presented in [74], which I co-authored. The chapter reproduces some text from [74] but any shared text between this chapter and the manuscript is text that I have originally written. I contributed in the early stages of the design of the electronics for the integrated homodyne detector, while the actual PCB design is due to fellow Ph.D student Giacomo Ferranti. I worked in collaboration with Giacomo Ferranti in the characterisation of the integrated homodyne detector. I led the part concerning the generation and characterisation of the quantum random numbers and the measurement and characterisation of coherent states. In collaboration with Giacomo Ferranti we developed a Matlab version of the maximum likelihood algorithm, as proposed in [60], used for the characterisation of the coherent states. Giacomo Ferranti led the characterisation of the photodiodes and the characterisation of the coupling losses. Jake Kennard developed the Toeplitz extractor used for the hashing of the random numbers. The photonic design was

realised by Alberto Santamato, Gary Sinclair and Damien Bonneau. Philip Sibson contributed in relation to the generation of quantum random numbers. Dylan Mahler and Jonathan Matthews supervised the whole experiment.

3.1 Introduction

Since its invention in the late decades of the 20th century, balanced homodyne detectors (BHD) have found use in diverse fields of classical and quantum optics (See [22] for a review and Refs. [75–79] for more recent achievements). In 1993 Smithey et al. for the first time were able to demonstrate sub-shot noise measurements of the optical electromagnetic field [80]. A few years later, at the beginning of the 21st century, A.I. Lvovsky and co-workers characterised single photons by using a homodyne detector. For the first time the negativity in the Wigner function of the quantum electromagnetic field described in the phase space, was observed [59]. Following these pioneering achievements, many other optical quantum states were observed and manipulated by using homodyne detectors. Of particular interest, in 1998 the first continuous-variable teleportation of quantum states was realised [81]. At the same time, continuous-variable based Quantum Computation (QC) and Quantum Key Distribution (QKD) emerged. On one side, a model for a quantum computer based on continuous-variable quantum states was developed [82]. On the other side, almost twenty years after the original proposal of Bennett and Brassard [83] based on discrete-variable, a scheme to perform QKD using continuous-variable and thus BHDs, was proposed by Grosshans [84]. More recently, homodyne detectors were also used to perform protocols [23, 24], to generate random numbers by measuring vacuum states.

However, beside these great achievements of the last few years, the complexity of these experiments has been limited by the costs and size of the components involved. In addition, homodyne detectors have the requirement of phase stability between the local oscillator and signal. In fibre and bulk optics, active control on the phase is therefore required. This means that when increasing the complexity of

the experiments controlling the phase of many homodyne detectors could become really hard. Integrated photonics can help solve most of these problems related to complexity and active stabilisation. Given the size of integrated components, many integrated homodyne detectors could be parallelised in a single, compact device. Besides, thanks to the monolithic nature of these microchips, the need for active stabilisation can be strongly reduced.

Here we report the demonstration of a homodyne detector integrated into the Silicon-on-Insulator platform able to characterise quantum states and generate random numbers at a high rate. With this device we aimed to open up a new way of using homodyne detection measurements that is low-cost and scalable.

Paper	Year	Experiment Description
[80]	1993	Squeezed State Measurement
[81]	1998	Teleportation of a Coherent State
[82]	1999	Continuous Variable Quantum Computation
[59]	2001	Single Photon Wigner Function
[84]	2003	Continuous Variable QKD
[85]	2004	Single Photon Added Coherent State
[86]	2007	Optical Schrödinger Cat
[75]	2010	Quantum-optical state engineering up to the two-photon level
[76]	2013	Continuous Variable Cluster States
[77]	2015	Continous Variable Entanglement on a chip

TABLE 3.1: ***Relevant experiments requiring homodyne detection.*** *We report a list of a few relevant experiments requiring homodyne measurements.*

3.2 Description of the experimental setup

The experimental setup used for this experiment is reported in Fig. 3.1. The laser source was a Yenista Tunics T100S-HP. It was fibre coupled to a 99% transmittivity beam-splitter, and both outputs were connected to fibre based polarisation controllers, to optimize the optical power coupled on-chip. The transmitted beam was used as local oscillator (LO) and vertically coupled into the chip via a V-groove array (VGA). The reflected beam was injected into variable optical attenuator (VOA) and a fast phase modulator (PM). This channel was used during the measurements

of coherent states (Section 3.4), while it was unplugged during the characterisation of the homodyne detector (Section 3.3) and for the generation of random numbers (Section 3.5). The photonics for the reported device (Fig. 3.1b) were fabricated on an SOI chip as part of a multi-project wafer run organised by IMEC foundry services [53][1]. The beam-splitting operation was performed by a multi-mode interference device (MMI) with two single-mode input waveguides and two single-mode output waveguides. Each of the output waveguides was coupled to an on-chip Germanium photodiode. The electronic signals generated by the photodiodes were then processed on a printed circuit board (PCB) by amplifying the difference of the two photocurrents. The design of this circuit was based on the one developed in [87], and details are included in the Methods chapter. The entire system, inclusive of the silicon chip and the PCB, was a few centimetres square and the total footprint of the integrated photonics was < 1 mm^2.

3.3 Homodyne detector characterisation

A real homodyne detector is characterised by imperfections leading to different sources of noise. In general, the global detection efficiency is given by the product of all of these individual contributions:

- Non-perfect efficiency of the photodiodes;
- Losses in the optical channels;
- Imbalance and losses at the beam-splitter;
- Electronic noise leading to limited signal-to-noise ratio.

These contributions can all be modelled as optical losses in the channel of the signal field and ultimately as a limiting factor for the detector efficiency. This is well described in [88] and reported in Appendix 3.10. A further issue is related with

[1]Details in Appendix 3.11.

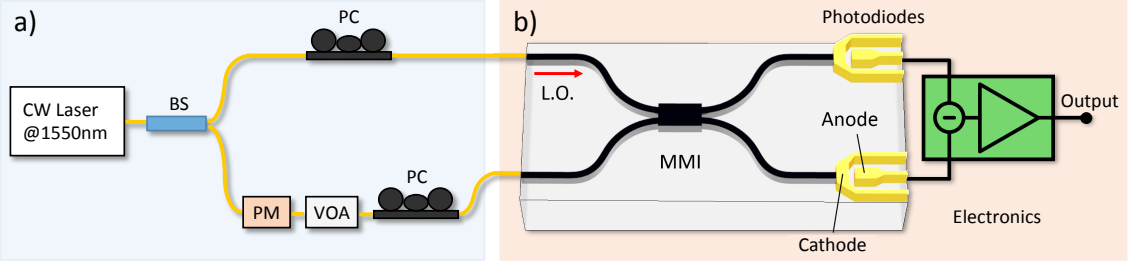

FIGURE 3.1: ***Schematic of the setup.*** *a) Setup for optical input characterisation. The laser source is a CW laser working at 1550 nm. BS refers to a 99/1 beam splitter which sends 99 % of the light on the LO channel and the remaining fraction into the signal channel. Both channels have a polarisation controller (PC) to optimise the power coupled into the integrated waveguides. On the signal channel there is also an off-chip phase modulator (PM) and a variable optical attenuator (VOA). These are used when performing the tomography of coherent states, in order to tune the amplitude and phase of the coherent states. During the characterisation of the detector and for generating quantum random numbers the bottom channel was disconnected, so no light was coupled inside the chip through the bottom port. The LO and the optical signal field are coupled into the waveguides. b) The silicon photonics homodyne detector. The beam-splitting operation of the integrated homodyne detector is performed by a multi-mode interferometer (MMI). The two outputs of the MMI are coupled into two on-chip Ge photodiodes, generating two currents that are subtracted from each other and amplified by an off-chip transimpedance amplifier (TIA).*

mode mismatch betweent the LO and the signal [87]. We note here that in integrated photonics, because of the high accuracy of the single mode waveguides, the LO and signal are inherently spatially mode-matched.

3.3.1 Characterisation of the photodiodes

In our experiment, the quantum efficiencies of the photodiodes were characterised by means of two effective responsivities taking into account the intrinsic responsivity of the photodiodes and the optical losses in the integrated beam-splitter (considering that the linear losses for the waveguides do not contribute substantially in this case). We obtained a value of (0.80 ± 0.07) A/W for one photodiode (Fig. 3.2a) and (0.78 ± 0.06) A/W for the other (Fig. 3.2b), corresponding to an estimated

quantum efficiency of $\eta_{pd} = 0.64 \pm 0.05$. Here we note that in order to estimate the efficiency of the system composed of MMI and photodiode we carefully estimated the coupling losses of the grating coupler. This was done by measuring many test structures in different copies of the same chip, for around 20 characterised structures. This procedure gave us a good level of confidence in the quality of the measured coupling losses and the standard deviation reported in the responsivity has as a main contribution the coupling uncertainty of the grating couplers.

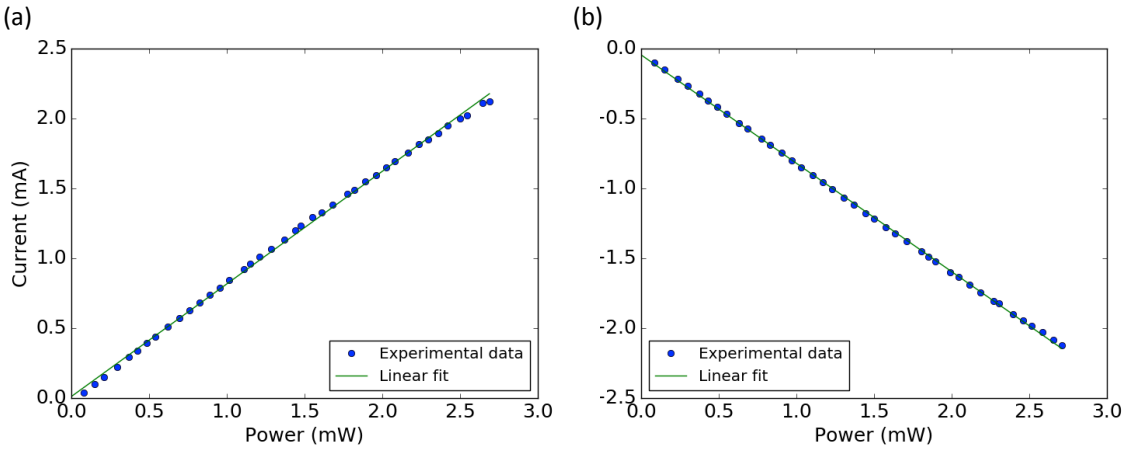

FIGURE 3.2: **Photodiodes characterisation.** (a) *Response of the photodiode generating a positive current, showing a responsivity of* 0.80 ± 0.07 *A/W.* (b) *Response of the photodiode generating a negative current, showing a responsivity of* 0.78 ± 0.06 *A/W.*

3.3.2 Common Mode Rejection Ratio (CMRR)

Another important parameter of homodyne detectors is the *Common Mode Rejection Ratio* (CMRR). It describes how well a homodyne detector is able to perform the subtraction between the two photocurrents. In the ideal case of perfectly equal photodiodes and for an ideal transimpedance amplifier the CMRR is infinite. However, mismatch in the photodiodes response and imperfect TIAs reduce the quality of the signal output by the homodyne detector. This causes reduction in the efficiency and affects the measurements of quantum states. In Fig. 3.3 we report the measurement of the CMRR for the homodyne detector. The CMRR is obtained as

the ratio (in logarithmic scale), between when the light is sent to a single photodiode, while the beam into the other photodiode is blocked and the signal when the light is sent to both photodiodes. A high value of the of the CMRR means that the signal into the two photodiodes have been subtracted well. Given the monolithic nature of our device, where the photodiodes are integrated with the waveguides, in order to measure the CMRR it was necessary to cut the electrical trace from one of the two photodiodes into the operational amplifier. The measurement was performed with a Pritel pulsed laser with 50 MHz repetition rate and operated at an optical power P = 18 μW. This very low power is necessary in order not to saturate the operational amplifier when detecting light from a single photodiode. A CMRR of 28 dB was measured, as can be observed from Fig. 3.3.

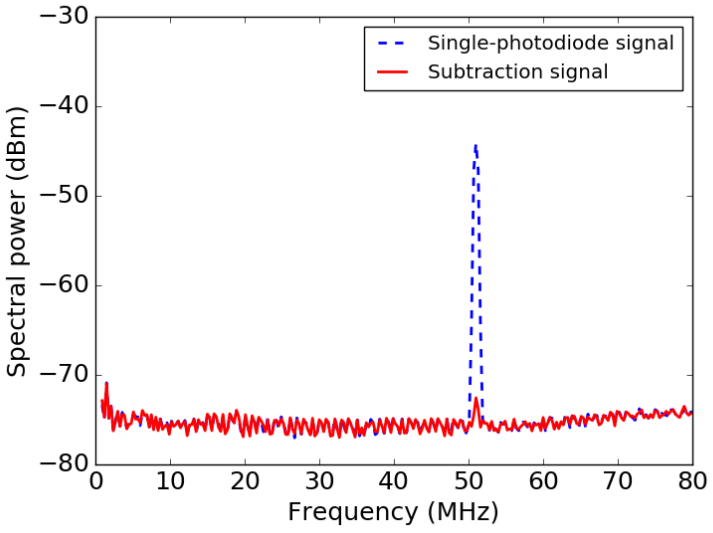

FIGURE 3.3: ***CMRR of the on-chip homodyne detector.*** *The blue dashed line represents the signal when just one photodiode is connected, while the red line represents the signal when both the photodiodes are connected.*

3.3.3 Efficiency of the Homodyne Detector

In order to estimate the efficiency of the homodyne detector, the signal-to-noise clearance (SNC) had to be determined. The SNC is related to the efficiency of the

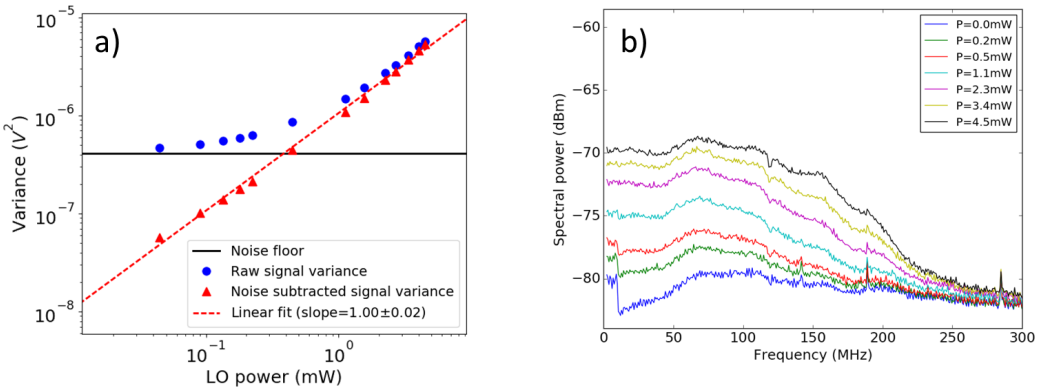

FIGURE 3.4: ***Performance of the on-chip homodyne detector.*** *(a) Signal variance for different LO powers, obtained with a CW laser at 1550 nm (Tunics T100S-HP). The blue dots represent the raw signal variances, the red triangles correspond to the noise-subtracted variances and the black line marks the variance of the electronic noise. The red dashed line is a linear fit of the noise-subtracted variances with slope of* 1.00 ± 0.02. *(b) Spectral response of the integrated homodyne detector for different LO powers, measured with a CW at 1550 nm (Tunics T100S-HP). The graph shows a SNC of 11 dB for a LO power of* (4.5 ± 0.4) *mW over a bandwidth of* $\sim$*150 MHz. These values have been measured using a CW LO at a wavelength of 1550 nm.*

homodyne detector by [87]

$$\eta_{SNC} = 1 - \frac{\sigma_{EN}^2}{\sigma_O^2}. \tag{3.1}$$

To obtain the SNC, the output of the homodyne detector was measured in absence and presence of the LO field. Given that both the electronic background noise and the shot-noise obtained by injecting the LO have a Gaussian distribution and are uncorrelated, the estimated shot-noise variance is

$$\sigma_{SN}^2 = \sigma_O^2 - \sigma_{EN}^2, \tag{3.2}$$

where σ_O^2 is the variance of the raw output of the detector, σ_{SN}^2 is the extracted variance of the shot-noise contribution, the fundamental quantum noise of the light field. Here σ_{EN}^2 is the variance of the electronic technical noise contribution, obtained in absence of the LO.

Fig. 3.4a shows a plot of the variance of the signal measured by our detector for different powers of the LO. The line of best fit through the noise-subtracted variances on a bi-logarithmic scale is a line of slope 1.00±0.02. This is in agreement the with the expected manifestation of quantum vacuum fluctuations as Gaussian-distributed white noise. The ratio between the variance of the raw output of the detector measured at the highest LO power used (4.5 ± 0.4 mW) and zero LO power (i.e. the SNC) is ∼11 dB, which corresponds to an efficiency of $\eta_{SNC} = 0.93$ which, combined with the photodiodes contribution, leads to a total detector efficiency of

$$\eta = \eta_{pd} \times \eta_{SNC} = 0.59 \pm 0.05.$$

It can be shown that this value is sufficient to characterise the quantum features of optical states [89, 90], as for example, the negativity of the Wigner function for single photons states in phase space [59].

Another main feature of a homodyne detector is the bandwidth. The bandwidth of a homodyne detector defines the speed at which it can be maximally operated and the maximum spectral width that the signal field can have in order to be measured efficiently. Moreover, in the specific application of the homodyne detector as a quantum random number generator, the bandwidth determines the maximum sampling rate of the device, and hence it defines the final generation rate of the QRNG. The measured spectral response of our detector is shown in Fig. 3.4b and the 3 dB bandwidth is ∼150 MHz.

3.4 Measurements of coherent states

Coherent states (displaced and Gaussian states in general) are amongst the main resources for CV quantum computing [82] and CV quantum communications [84]. For example, in CV QKD a sender shares a secret key with a receiver by encoding two randomly selected real variables x and y in a displaced coherent state described in the phase space by $|x + iy\rangle$. These states are sent to the receiver who performs

homodyne measurements on the quadratures in order to extract the secret key. Therefore homodyne detectors capable of characterising displaced Gaussian states are one of the main tools when performing CV based QKD. In the phase-space, coherent states are described as displaced 2D Gaussian distribution as

$$W(\hat{Q},\hat{P}) = \frac{1}{\pi}\exp\left[-(\hat{Q}-Q_0)^2+(\hat{P}-P_0)^2\right], \tag{3.3}$$

obtained by setting $\hbar = 1$. Q_0 and P_0 represent the projection of α respectively onto the Q and P axis.

The detector's capability in performing homodyne tomography was demonstrated using the full arrangement displayed in Fig. 3.1. As previously mentioned, a 1550 nm continuous wave laser with 2.5 μs coherence time (Tunics T100S-HP) was split at a fibre beam-splitter with 1 % reflectivity. The reflected beam was further attenuated by a variable optical attenuator, phase-modulated by means of a fibre phase shifter and then injected into the chip. (see Fig. 3.1). The transmitted beam was used as a local oscillator. Quadrature measurements in a phase interval of length π were acquired by driving the phase shifter with a triangle wave sweeping the interval at a frequency of 200 kHz. The entire set of data was acquired within a time interval of 40 μs, significantly shorter than the time scale of phase instabilities of the optics external to the SOI chip ($\sim$ 150 μs). Quadratures were sampled at 145 Msamples/s. We notice here that the integration of a homodyne detector on a monolithic SOI device does not solve yet the issue of phase stability between the local oscillator and the coherent signal. In fact, given that the splitting between the LO and the coherent beam is performed off-chip, any change in phase that happen off-chip would affect the phase stability regardless if the homodyne detector is integrated or not. Indeed, the main motivation for this measurements was to show the capability of the homodyne detector to measure displaced states, fundamental in almost any protocol based on continuous-variable. An on-chip solution to the phase instability would require the splitting between local oscillator and coherent beam to be performed on-chip. This is not a trivial task given the very fine splitting quality required to pass from optical powers of a few 5-10 mW for the LO to the few photons per mode of a weak

coherent state. However recently splitting up to 60 dB has been demonstrated for MZI integrated in Silicon [91]. This approach paves the way of integrated splitting and therefore intrinsically phase stable homoydne detector (at least in the context of coherent states).

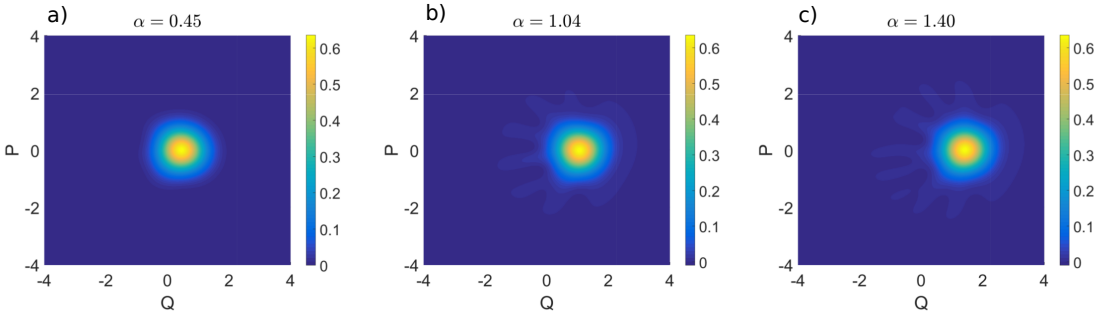

FIGURE 3.5: ***Experimental Wigner function for coherent states.*** *Measured coherent states with amplitude values (a) $\alpha = 0.45$, (b) $\alpha = 1.04$ and (c) $\alpha = 1.40$. We chose to set the phase such that $Im(\alpha) = 0$. The fidelities with the ideal state are respectively $\mathcal{F}_{0.45} = (99.57 \pm 0.31)\%$, $\mathcal{F}_{1.04} = (99.31 \pm 0.40)\%$ and $\mathcal{F}_{1.40} = (99.13 \pm 0.67)\%$.*

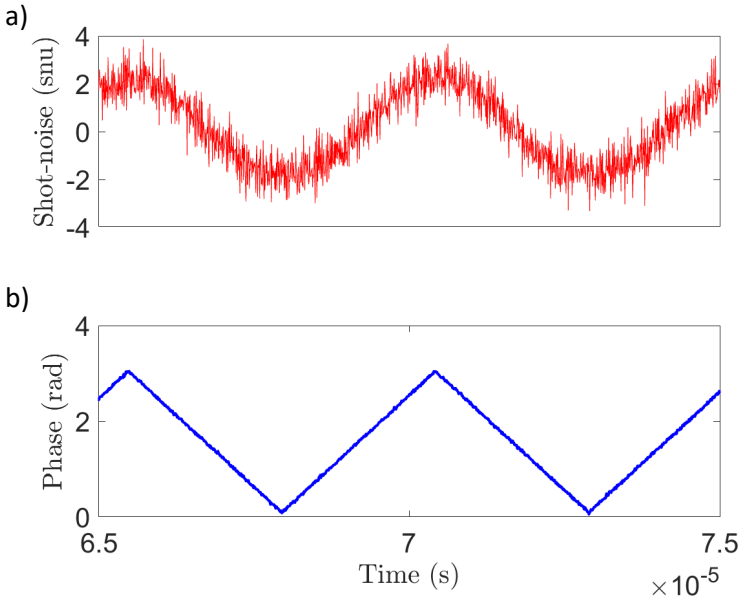

FIGURE 3.6: ***Coherent state measured by the oscilloscope.*** *a) The coherent state is measured for different values of the phase, in a time interval of 10 μs. b) The phase modulation of the coherent state is achieved by taking advantage of a fast phase-modulator whose phase is varied between 0 and π.*

The Wigner function of the state was then reconstructed using an iterative maximum-likelihood reconstruction algorithm taking into account the reduced efficiency of the detector and the uncertainty on the coupling losses [60]. In Fig. 3.5 we reported the characterisation performed for three different amplitude values of the coherent state, α: 0.45, 1.04, 1.40. (In Fig. 3.6 we report the measured coherent state in a time window of a 10 μs). The quantum state fidelities obtained in the three cases were respectively $\mathcal{F}_{0.45} = 99.57\% \pm 0.31\%$, $\mathcal{F}_{1.04} = 99.31\% \pm 0.40\%$ and $\mathcal{F}_{1.40} = 99.13\% \pm 0.67\%$. The quantum fidelity between the experimental data and the ideal density matrix was calculated by setting $\alpha_{\text{sim}} = \alpha_{\text{exp}} \pm \Delta P$, where ΔP takes into account the uncertainty on the coupling losses and on the efficiency of the detector. The fidelity was taken as the mean of the fidelities of 100 different sets of simulated data. The standard deviation was obtained as the standard deviation of these fidelities. The calculated fidelities are respectively $\mathcal{F}_{0.45} = 99.57\% \pm 0.31\%$, $\mathcal{F}_{1.04} = 99.31\% \pm 0.40\%$ and $\mathcal{F}_{1.4} = 99.13\% \pm 0.67\%$. Therefore these fidelities show that the homodyne measurements preserve the Gaussian shape of the coherent states' Wigner function on the phase-space. Alternatively, instead of generating the simulated coherent states starting from the measured α_{exp}, a possible solution would have been to estimate α by taking into account the splitting ratio, the attenuation at the VOA, the optical losses inside the chip. However, having an accurate estimation of these parameters was not feasible in our experimental condition and hence we opted for the method described above.

3.5 Generation and certification of random bits

Random numbers are a key resource for quantum cryptography, as well as classical cryptography and have applications in more general computational simulation and fundamental science.

However true randomness cannot be generated with a classical computer—currently used pseudo-random numbers generated with software can in principle be predicted. In contrast, quantum random number generators (QRNGs) rely on the outcomes of

inherently non-deterministic quantum processes to generate random numbers that cannot be predicted [15, 24, 26, 34, 92]. Examples of compact QRNGs have been recently demonstrated [40–43]. To the best of our knowledge, our report is the first experimental demonstration in the SOI platform. The quadrature measurements $\hat{Q}$ for the vacuum states are non-deterministic and follow a Gaussian probability distribution

$$P(\hat{Q}) = \frac{1}{\sqrt{\pi\hbar}} e^{\frac{-\hat{Q}^2}{\hbar}}, \tag{3.4}$$

as shown in Fig. 3.7. They were obtained by injecting the LO beam into the top waveguide in Fig. 3.1, while blocking the bottom waveguide. To extract the random bits, the voltage output of the homodyne detector was read by an oscilloscope, in windows of 10^5 samples. The range of measurements of the vacuum states were divided into 2^8 equally spaced bins, and each bin was labelled with an 8−bit string, similarly to Fig. 3.7[2]. Thus each measurement outcome corresponded to the generation of an 8−bit number. To be compatible with randomness extraction hardware we used equally spaced bins, but this means the bits strings associated with the

[2]In Fig. 3.7 we are using 3−bit string, and we are dividing the range into $2^3 = 8$ bins.

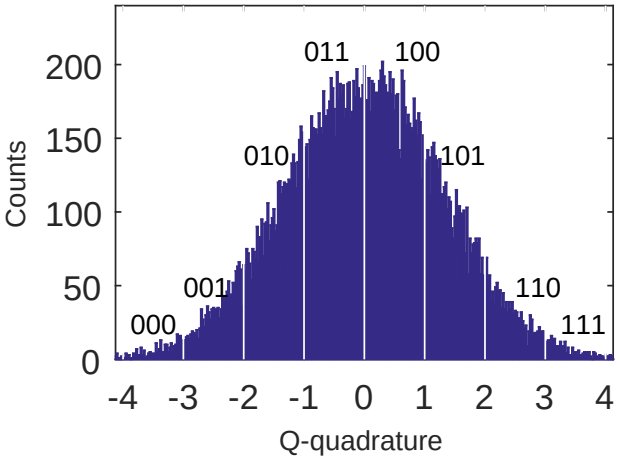

FIGURE 3.7: ***Measured histogram of the shot-noise signal.*** *The quadratures have a Gaussian distribution. The corresponding shot-noise histogram is divided into 2^n bins and each bin is labelled with a n-bit string which is used to label each sample from the oscilloscope. Since the outcomes are unpredictable, a bit string composed of all the samples will be random. We illustrate with n=3 bits as an example.*

central bins were more likely to appear, skewing the randomness of the random bits. Moreover, correlations in the electronic background noise could be used by an adversary. For this reason a further step of randomness extraction from the raw data was required. We implemented the Toeplitz hashing algorithm [65] as a randomness extractor with a desktop computer (described in Chapter 2.4.2.2). The output of the Toeplitz algorithm was a sample of bits characterised by a uniform distribution, where the residual correlations between the raw random data have been removed. We then estimated the generation rate of quantum random numbers for our homodyne detector. First we note that our sequences were acquired at a rate of 200 Msamples/s. Moreover, we estimated the amount of certified randomness of the generated bits by calculating the min-entropy [65], obtaining $H_\infty = 5.9$ bit/sample. Finally the calculated generation rate was 1.2 Gbps, obtained as the product between the calculated min-entropy of 5.9 bits/sample and the sampling rate of 200 Msamples/s. Here we note that since we acquired the data with an oscilloscope and used a software based Toeplitz algorithm, the randomness extraction was performed off-line. However, this estimation gives information about the capabilities of the detector itself and the obtained generation rate is the direct result of the combination of SNC and bandwidth of our homodyne detector. Hardware based randomness extractors could be used to improve the generation rate [31, 92]. We then tested the generated random bits with the NIST SP 800-22 statistical tests provided in Ref. [93]. Our QRNG passed all the tests provided. In Table 3.2 we report the results for the NIST SP 800-22 statistical tests. Fig. 3.8 shows the results for the uniformity tests on the P-values.

3.6 Randomness Extraction

The Toeplitz hashing algorithm takes a k-bit string of raw bits obtained by binning the random data from the oscilloscope and multiplying it by a $k \times j$ Toeplitz matrix, giving as a result an unbiased j-bit random string [65]. Here j is given by the length of the input sequence of bits times the ratio between the H_∞ and number of bits

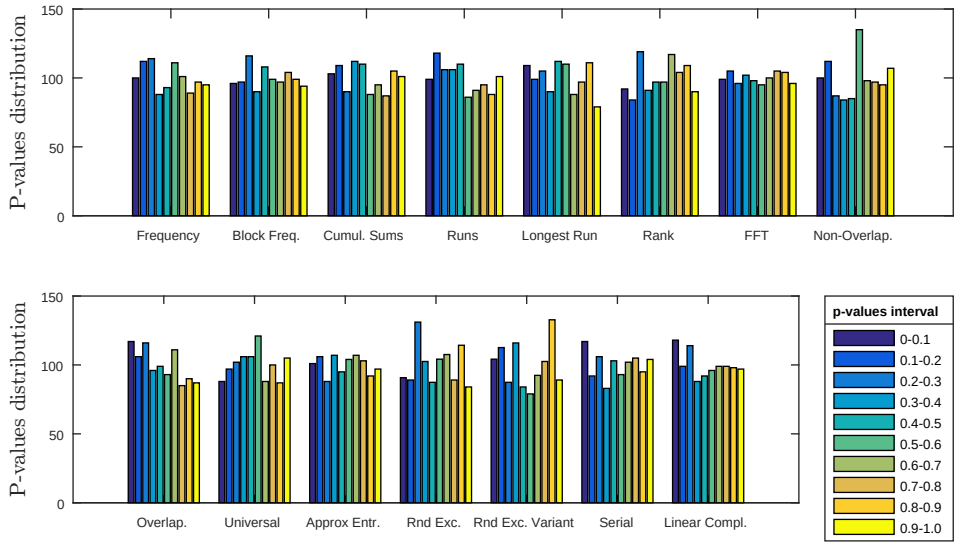

FIGURE 3.8: ***Uniformity test for the P-values.*** *Under the assumption that the produced random bits are truly random, the P-values must be uniformily distributed between 0 and 1. Here the NIST statistical test provides the frequencies of the P-values, by dividing the (0,1) interval into 10 sub-intervals. We can observe that for each test the P-values are uniformly distributed.*

NIST SP800-22		
Test name	Pass Rate	P-value
Frequency	0.996	0.524
Block Frequency	0.998	0.827
Cumulative Sums	0.994	0.536
Runs	0.990	0.397
Longest Run	0.990	0.233
Rank	0.990	0.178
FFT	0.987	0.998
Non Overlapping Template	0.990	0.012
Overlapping Template	0.991	0.180
Universal	0.992	0.344
Approximate Entropy	0.987	0.910
Random Excursions	0.993	0.214
Random Excursions Variant	0.995	0.082
Serial	0.989	0.528
Linear Complexity	0.989	0.574

TABLE 3.2: ***Statistical tests on the random data.*** *Here the results for the NIST (National Institute of Standards & Technology) statistical tests suite [93]. In order to pass the NIST SP800-22 the pass rate must be above 0.98 for each type of test (column II) and the reported P-values, which refer to the uniformity test on the distributions plotted in Fig. 3.8, must be above 0.01 (column III).*

used (8 bits in our case). Hence, in order to extract pure random bits, for each sequence we estimated the min-entropy which describes the amount of extractable randomness from the quantum signal distribution. It is defined as

$$\mathrm{H}_\infty = -\log_2(\max_{x\in\{0,1\}^n} \Pr[X = x]), \tag{3.5}$$

where X corresponds to the quantum signal shot-noise distribution over 2^n bins, and $Pr[X = x]$ is the probability to obtain a particular value for X[3]. In homodyne detection however, we do not have direct information about the quantum signal distribution because it is always mixed with some classical noise. We thus estimated the true quantum variance under the assumption of a Gaussian distribution, using Eqn. 3.2. For each sequence we calculated a min-entropy of $H_\infty \sim 5.9$ bits/sample and then built a Toeplitz matrix, using a pseudo-random seed of k+j-1 bits as in Ref. [65]. An alternative approach could be to substitute part of this pseudo-random seed with a certified random string, obtained by previous experiments. Finally the raw sequence of bits was multiplied by the Toeplitz matrix to obtain the unbiased random sequence.

3.7 Autocorrelation of the random bits

As a test of randomness we calculated the bit-string autocorrelation. We used 8-bit samples to plot the autocorrelations, reported in Fig. 3.9. The autocorrelation of a sample is written as

$$R(\tau) = \frac{E\left[(x_i - \mu)\,(x_{i+\tau} - \mu)\right]}{\sigma^2}, \tag{3.6}$$

where $E[\cdot]$ is the expectation value, μ is the mean, σ^2 is the variance and τ is the shift, usually expressed either in samples or in time units. Ideally, for a independent and randomly distributed samples, the function R(τ) is zero for every $\tau \neq 0$ and it should be equal to one for $\tau = 0$. However, in the realistic case of a finite number of samples and a limited resolution of the system, the value of the autocorrelations

[3] Eq. 3.5 is valid under the assumptions described in [65] and reported in Section 2.4.2.1.

will be small but never zero. Peaks and oscillations in the autocorrelation function indicate that the random bits are not *independent and identically distributed* (iid), and therefore partially predictable.

Correlations in the samples can be due to a wide range of causes. The most obvious cause could be the environmental noise peaked up by the electronics and amplified by the transimpedance amplifier (TIA). The main contribution for our experiment is the FM radio signals around 100 MHz. As a countermeasure for this, a solution is a carefully shielded apparatus, obtained for example by building a Faraday cage. This was the method implemented in this experiment and details can be found in Chapter 6. Other causes are related with the digitization process of the analog signal in output from the TIA. These are a consequence of a limited bandwidth of the homodyne detector. A detailed analysis of the effect of the limited bandwidth in relation with the sampling rates was done in [25, 94].

In Fig. 3.9a we plot the autocorrelation for the raw data at different sampling rates. While increasing the sampling rate up to 1 Gbit/s clearly introduces correlations, sampling at 200 Msamples/s does not show higher correlation compared to, for example, the 125 Msamples/s sampling. This is because the quantum noise is well above the electronic noise level up to 200 MHz. Thus, a sampling rate of 200 Msamples/s is justified. Moreover the hashed data do not present any significant correlation here, as shown in Fig. 3.9b.

3.8 NIST statistical test

We applied the NIST SP 800-22 test to a sequence of 10^9 random bits. This provides 15 different tests. For each test the total string of random bits was divided into 1000 blocks. All the tests were applied to each block (with the exceptions of the Random Excursion and Random Excursion Variant tests, which use approximately 600 blocks), and a P-value was extracted for each single test. These P-values describe the probability to obtain a more biased string of bits than the one obtained, under

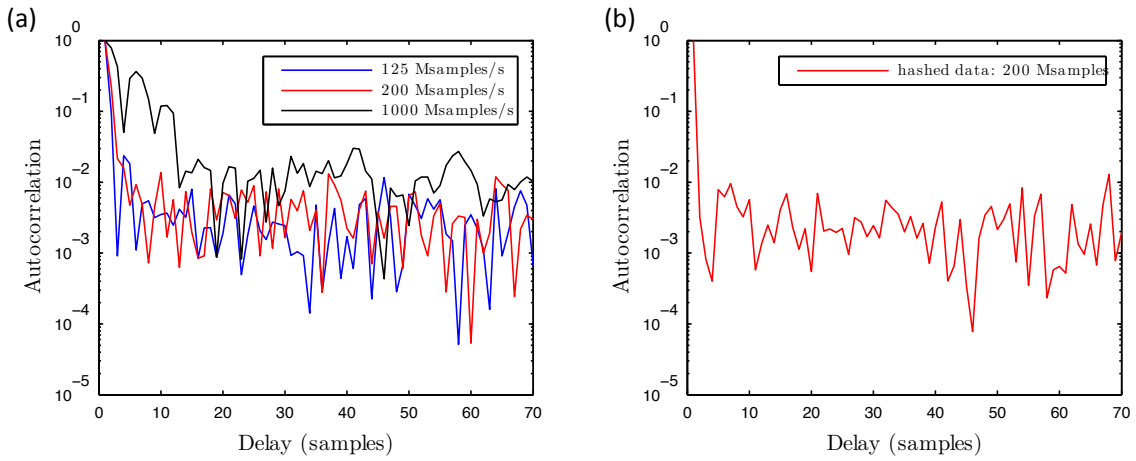

FIGURE 3.9: **Autocorrelations.** (a) The autocorrelation of the raw bits string of random data at different sampling rates. The autocorrelations at the sampling rates of 1 Gsamples/s, 200 Msamples/s and 125 Msamples/s are shown respectively as black, red and blue solid lines. The autocorrelation has a larger magnitude for a sampling well above the detector bandwidth, but decreases when the sampling is 200 Msamples/s or below. (b) The autocorrelation of the bits string after the Toeplitz Hashing at 200 Msamples/s. 8×10^4 8-bit samples were used to calculate these autocorrelations.

the assumption that the bits are the outcomes of a perfect quantum random number generator. In order to assess the randomness of the data, there are two requirements specified by NIST SP 800-22 test. First, the proportion of single tests with a P-value greater than 0.01, reported in the second column of Table 3.2, must be above 0.98. Second, by definition of P-value, the P-values obtained from all the single tests must be uniformly distributed. Thus, a second set of P-values was calculated to assess the uniformity of the distributions original P-values. These final P-values, one for each of the 15 tests, must be above 0.01 to confirm the randomness of the data. In Fig. 3.8 we plotted the P-values distributions for the different tests. As can be observed, the P-values are uniformly distributed, indicating the randomness of the experimental data. In the third column of Table 3.2 the P-values for the uniformity tests are reported.

3.9 Discussion

With this experiment we reported a homodyne detector integrated on an SOI chip. Our device showed more than 10 dB shot-noise to electronic noise clearance, an efficiency of 60% and a bandwidth of 150 MHz. These specifications are sufficient to observe the quantum features of optical states, such as, for example, the negativity of the Wigner function for single-photons [59]. As first applications, we generated quantum random numbers based on vacuum states at a Gbps rates and measured optical coherent states.

The photonic part of the homodyne detector is characterised by high efficiency, high-speed photodiodes, low-loss waveguides and an integrated beam-splitter. In this case, a thermo-optic phase-shifter could be introduced to control the phase of the LO on-chip, with low losses. Faster carrier-depletion phase-modulators are available in silicon. However these are characterised by considerable losses (4-6 dB) [53, 55]. The choice on the kind of phase modulator will depend on the specific experiment.

When generating random numbers, a fast, integrated phase-shifter would enable source-independent schemes, where controlling the phase of the local oscillator beam is required [28–30]. When measuring coherent states (and quantum states in general) an integrated phase-shifter would be even more relevant. For example, when we performed the measurement of coherent states, given that the phase-shifter was off-chip, phase instabilities were still present in our measurements. The way we overcame this issue was taking measurements within a time interval where the phase was stable. However, while during the measurement there was phase stability between local oscillator and coherent signal, their relative phase was not controlled and we manually took measurements where their relative phase was zero. Therefore, in our case, the monolithic nature of the photonic chip did not provide a complete solution to the phase instabilities. Also, in the context of phase-dependent measurements of quantum states, an integrated phase-shifter would not provide a complete solution as it is the relative phase between the local oscillator and the signal beam that

must be stable. In some cases such as coherent states quantum process tomography, where coherent states are the only requirement to characterise quantum circuits, a possible solution could be the generation of the coherent states by splitting the local oscillator. This of course would require an extremely fine control of the splitting ratio, in order to pass from the characteristic powers of a few milliwatts of the local oscillator to a few photons per mode of a weak coherent state [91].

In terms of integrated components, here we had a 50% multimode interferometer as an integrated beam-splitter. Therefore, we did not have control in the ratio between the outputs. This implies that we had no chance to control and correct for the little discrepancy between the responsivity of the two photodiodes. A possible solution would be to implement a Mach-Zehnder interferometer composed of two MMIs connected by a phase-shifter. However this would reduce the efficiency, given that the MMIs have excess losses (0.5 dB each). An alternative solution could be to substitute the MMIs with directional couplers, which have negligible losses. These however have a smaller bandwidth and are very sensitive to temperature changes. Therefore, depending on the specific application one might prefer single beam-splitter or tunable MZI, based on MMIs or directional couplers.

Comparing the generation rate of our device with some results present in the literature, we see that their demonstrations are more than one order of magnitude faster than our QRNG [29, 30]. Ultimately, the two parameters that determine the generation rate are the signal-to-noise clearance (SNC) and the bandwidth of the homodyne detector used. Therefore the different results are explained in terms of these two parameters. In particular, both the cited demonstrations use off-the-shelf balanced detectors with a bandwidth of 1.5 GHz. However, these faster balanced detectors are characterized by a higher electronic noise, and so to achieve an SNC similar to our detector they have to use a brighter local oscillator. This is possible because they take advantage of bulky photodiodes that saturate at higher input optical powers. On the other hand, given that the extractable randomness varies only with the logarithm of the SNC, by improving the bandwidth of the detector at the cost of a lower SNC, it would be possible to improve the generation rate

(we note here that our device was optimised to obtain the best efficiency and not the optimal rate of extractable randomness). In summary, the difference in generation rate is a combination of different factors that include the intrinsic bandwidth of the homodyne detector (and the underlying transimpedance amplifier) combined with its electronic noise, as well as parameters such as the saturation level of the photodiodes and the brightness of the laser source.

On the side of the transimpedance amplifier, many solutions are possible, always depending on the specific requirements. Our design is based on a commonly used operational amplifier [95], and thanks to the integrated photodiodes we almost reached the optimal performance for this device. Other solutions are present, as shown in [96] and more recently in [97], where higher bandwidths were achieved with high shot-noise clearance and flat spectral response. These solutions would potentially bring the generation rates beyond 10 Gbps.

Given the maturity of this QRNG, it could be deployed in the near future in real-world applications. An important aspect in this sense is to be able to compensate for all the possible failures of this device. Depending on the specific application, different levels of *security checks* could be applied. The aspects that mainly affect the generation of random numbers are the correct working of the photodiodes and amplification stage, as well as the CMRR (which determines the amount of bias towards either 0 or 1). Another important aspect is the level of influence that the environment introduces to the system. Because of the presence of high-speed amplifiers, it is very important to monitor the power spectral density of the quantum signal, to check for potential peaks in the spectrum. Background peaks comparable to the quantum shot-noise would introduce periodicity in the raw bit strings, destroying the intrinsic randomness of the quantum shot-noise. All the above checks can be applied simply by controlling the laser, the bias of the photodiodes and the input and output of the amplifier. This kind of control can easily be applied in real-time, either by periodically interrupting the generation of random bits to perform check measurements or by a careful design of the device. Other detrimental factors could be the presence of a malicious third party that could try to influence the outcomes

of the measurements by manipulating the devices when left untrusted. In this sense, recently source-device independent QRNG based on homodyne detection have been demonstrated [28–30]. These schemes, by measuring the q and p quadratures set a bound on the information that could be possessed by a malicious eavesdropper.

3.10 Appendix A: Efficiency Limitations in Homodyne Detection

Here we give an insight on the factors that limit the efficiency of homodyne detectors, as mentioned in Chapter 3. Ultimately, the efficiency determines how well a quantum state can be reconstructed with a homodyne detector. For example, considering single photons, the minimum efficiency required to observe the negativity of a Wigner function is $\eta_{tot} > 0.5$ [59]. In Chapter 3, the efficiency was written as a product of different contributions

$$\eta_{tot} = \eta_{PD} \times \eta_{SNC}, \tag{3.7}$$

where η_{PD} is the efficiency of the photodiodes and η_{SNC} is the efficiency reduction due to the electronic noise. We notice that in that case, given the impossibility of characterizing the efficiency of the photodiodes independently from the efficiency due to the linear losses inside the chip, η_{PD} takes into account also the losses to the waveguides and MMI.

3.10.1 Optical losses and photodiodes inefficiency

Any inefficiencies in the optical channel of the homodyne detector or in the photodiodes can be modelled by a beam-splitter with limited transmissivity placed in the optical channel itself. It can be shown [58] that for homodyne detection this is equivalent to placing at the input of the signal field. This as the consequence that the probability distribution for non-perfect detection is

$$pr(q;\eta) = \frac{1}{\sqrt{\pi(1-\eta)}} \int_{-\infty}^{\infty} pr(x) \exp\left[-\frac{\eta}{1-\eta}\left(x - \eta^{-1/2} q\right)^2\right] dx \tag{3.8}$$

3.10.2 Electronic noise and η_{SNC}

It can be shown that electronic noise in the amplification electronics has the same effect on the efficiency as the optical losses [88]. In particular, the marginal distribution of a quantum state, measured by a homodyne detector with non-zero electronic noise, has the same form as 3.8. This leads to the conclusion that any electronic noise affects the measurement as a lossy optical component and therefore the electronic noise contribution itself relates directly to the inefficiency. For clarity, here we derive this conclusion similarly to the method shown in [88].

We saw in Eq. 3.4 that the marginal distribution of the vacuum state is

$$P(\hat{Q}) = \frac{1}{\sqrt{\pi}} e^{-\hat{Q}^2}, \tag{3.9}$$

where here we put $\hbar = 1$. The variance of the distribution is therefore

$$\sigma^2 = \int_{-\infty}^{\infty} \hat{Q}^2 P(\hat{Q}) d\hat{Q} = \frac{1}{2}. \tag{3.10}$$

Then, we can write in a more general way

$$P(\hat{Q}) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{\hat{Q}^2}{2\sigma^2}}, \tag{3.11}$$

When performing homodyne detection measurements, the quantum signal is always mixed with electronic noise due to the measurement device itself. Specifically, the observed signal is the convolution of the actual quantum signal, that in the case of vacuum states is characterised by $\sigma = \frac{1}{2}$, and the electronic noise. The electronic noise is normally distributed as well, with variance $\sigma_{EN} > 0$

$$p_e(\hat{Q}) = \frac{1}{\sqrt{2\pi}\sigma_{EN}} e^{-\frac{\hat{Q}^2}{2\sigma_{EN}^2}}, \tag{3.12}$$

Therefore, the observed distribution becomes

$$P_{exp}(\hat{Q}) = \frac{1}{\sqrt{2\pi}\sigma_{tot}} e^{-\frac{\hat{Q}^2}{2\sigma_{tot}^2}}, \tag{3.13}$$

where $\sigma_{tot} = \sqrt{\sigma^2 + \sigma_{EN}^2}$.

This was obtained as the convolution of the quantum signal with the electronic noise

$$\begin{aligned} P_{exp}(\hat{Q}) &= \int_{-\infty}^{\infty} P(\hat{Q}) p_e\big(\hat{Q}' - \hat{Q}\big) d\hat{Q}' \\ &= \frac{1}{\sqrt{2\pi}\sigma_{EN}} \int_{-\infty}^{\infty} P(\hat{Q}') \exp\left[-\frac{1}{2\sigma_{EN}^2}(\hat{Q}' - \hat{Q})^2\right] d\hat{Q}'. \end{aligned} \tag{3.14}$$

Therefore, remembering the definition of efficiency η

$$\eta = \frac{\sigma^2}{\sigma_{tot}^2} = \frac{\sigma_{tot}^2 - \sigma_{EN}^2}{\sigma_{tot}^2} = 1 - \frac{\sigma_{EN}^2}{\sigma_{tot}^2}, \tag{3.15}$$

we obtain

$$\sigma_{EN}^2 = \sigma^2 \frac{1-\eta}{\eta}. \tag{3.16}$$

Finally, since $\sigma^2 = 1/2$, substituting $Q' = x/\sqrt{\eta}$ we get

$$P_{exp}(\hat{Q}) = \frac{1}{\sqrt{\pi(1-\eta)}} \int_{-\infty}^{\infty} P(\hat{Q}') \exp\left[-\frac{\eta}{1-\eta}(\eta^{-1/2}\hat{q} - \hat{Q}')^2\right] d\hat{Q}'. \tag{3.17}$$

Here we remark once more that the importance of this result is that it shows that the electronic noise due to the limited signal-to-noise ratio can be modelled exactly as if it were optical noise. Hence, this make it possible to consider the limited signal-to-noise ratio in the same way as optical losses/inefficiencies in the homodyne detector.

3.11 Appendix B: iSiPP25G Technology

The experiments described in Chapter 3 and 4 were performed using SOI chips provided by the IMEC foundry. These devices were manufactured by using the iSiPP25G technology, described in [53]. The coupling into the chip was obtained through the use of grating couplers. These had been characterised by connecting two grating couplers by a short waveguide, in such a way that the linear losses were orders of magnitude smaller than the coupling losses. The measured coupling losses were 3.5-4 dB per facet. The single mode waveguides were obtained by full etching of the silicon layer with a cross section of 450×220 nm. The Germanium photodiodes were grown by partially etching the silicon waveguides, and by reduced pressure chemical vapor deposition epitaxy. Our photodiodes had an estimated bandwidth of 23 GHz, with dark current < 30 nA and a responsivity R = 0.97. At 1550 nm, such responsivity means an efficiency of $\eta = 0.8$. The thermal phase-shifters used for the MZIs were obtained by an n-doped Silicon layer beside the waveguide, allowing a 2π shift in the phase of the MZI. The MZI were built by combining two multimode interferometers connected through a phase-shifter. The MMIs were estimated to have excess loss of $\alpha_l = 0.5$ dB and a similar imbalance.

Chapter 4

Integrated QRNG based on phase fluctuations from a diode laser

This chapter is based on the results presented in [98], which I co-authored. The chapter reproduces some text from [98] but any shared text between this chapter and the manuscript is text that I have originally written. In this experiment I led the experimental realisation and data analysis. Jake Kennard and Philip Sibson proposed the experiment and designed the photonic chip. Jonathan Matthews and Dylan Mahler supervised throughout the experiment.

4.1 Introduction

In the recent years, generation of random numbers based on quantum mechanical systems has been demonstrated exploiting different schemes, both in the discrete-variable and continuous-variable regime [1]. In the previous chapter we reported the demonstration of a silicon-on-insulator chip to generate random numbers based on homodyne detection. Homodyne based QRNGs have the advantage of requiring, in terms of optical components, simply a laser, a beam-splitter and two photodiodes. However, so far, the highest reported generation rate of quantum random numbers has been obtained by exploiting the phase fluctuations of laser diodes [34, 35]. These

results were achieved a few years after the first demonstration of this approach [33]. The method exploits a fundamental property of laser emission. For a laser, the emitted light is characterised by a contribution from the stimulated emission and a contribution from the spontaneous emission. Sometimes spontaneous emission is seen as a limitation as it is responsible for the limited coherence time of lasers. This can negatively affect optical communications based on amplitude-phase encoding [99]. However, spontaneous emission, characterised by random fluctuations in the phase, can be efficiently exploited to generate true quantum random numbers. It is this the scheme that we implement using silicon on insulator tehcnology, coupled to an external laser source. The scheme used to generate random numbers based on phase fluctuations from a laser diode exploits the fact that phase fluctuations can be mapped onto intensity fluctuations by an unbalanced Mach-Zehnder interferometer and these intensity fluctuations can then be detected by standard photodiodes. Therefore this technique makes use of readily available, low cost source and measurement devices and linear optics components. A similar approach to [33, 34] has been demonstrated in [36, 37, 41, 42]. In that case the randomness is obtained interfering subsequent pulses from a laser diode operated in pulsed regime. By switching the laser on and off, the relative phase between two pulses is random. Therefore interfering different pulses will have the effect of generating a random photocurrent signal when detected by a photodiode.

While an integrated laser source is not available yet in silicon, photodiodes, phase-shifters and beam-splitters are readily available in the SOI platform [53]. Moreover, the SOI platform enables the design of compact and intrinsically phase-stable devices, reducing the need of active phase-stabilisation. In this chapter we report the demonstration of a QRNG based on phase fluctuations, where all the optical and opto-electronic components are integrated onto a SOI device. Our compact device shows good phase-stability combined with low optical power operation.

The theory behind this QRNG can be found in Refs. [33, 34]. The electromagnetic field of the emitted light from a laser diode can be expressed as

$$E(t) = Ee^{-i(\omega t+\theta(t))}, \tag{4.1}$$

where ω is the angular frequency of the electromagnetic field and $\theta(t)$ is a random phase due to the contribution of the spontaneous emission of the emitted light [99, 100]. In Section 4.11 a more detailed description of the origin of the random phase fluctuations is described. In order to take advantage of the random phase fluctuations of the electromagnetic field, the light is injected into an unbalanced Mach-Zehnder interferometer (MZI). For a 50:50 perfectly balanced beam-splitter and lossless optical channels the intensity at the photodiodes can be written as

$$I(t) = 2E^2 + 2E^2\cos[\omega\tau + \theta(t+\tau) - \theta(t)], \tag{4.2}$$

where τ is the time delay between the two arms of the interferometer. Removing the phase independent term[1] the intensity can be written as

$$I(t) = Pcos[\omega\tau + \Delta\theta(t)] = P[\cos(\omega\tau)\cos(\Delta\theta(t)) - \sin(\omega\tau)\sin(\Delta\theta(t))], \tag{4.3}$$

where $\Delta\theta(t) = \theta(t+\tau) - \theta(t)$. This can be expressed as

$$I(t) \propto P\sin(\Delta\theta(t)) \sim P\Delta\theta(t), \tag{4.4}$$

where the first equality holds when the phase delay due to the different length between the two arms of the MZI is $2m\pi + \pi/2$, and the second relation is valid for small values of $\Delta\theta(t)$. The light intensity at the photodiodes is converted into voltage by a transimpedance amplifier and the variance of the voltage measured by the oscilloscope can be expressed as

$$\sigma^2 \equiv \langle\Delta V(t)^2\rangle \propto AP^2\langle\Delta\theta(t)^2\rangle + F. \tag{4.5}$$

[1]This is practically achieved by inserting a high-pass filter after the fast photodiode (not shown in Fig. 4.1).

Here $\langle \Delta\theta(t)^2 \rangle$ is the variance of the phase noise, A is the conversion factor between the optical power into the voltage which takes into account the responsivity of the photodiodes and the gain of the transimpedance amplifier that converts the photocurrent into voltage. P is the optical power and F is variance of the background electronic noise. It can be shown [99–101] that the variance of the random phase of a diode laser is the sum of an intrinsic quantum phase noise and a classical phase noise and it can be expressed as

$$\langle \Delta\theta(t)^2 \rangle = (\frac{Q}{P} + C), \tag{4.6}$$

where Q describes the intrinsic contribution given by the spontaneous emission and therefore describes the *quantum* contribution, while C is due to the phase-fluctuations that induced by classical effects. As a consequence, the variance of the voltage becomes

$$\sigma^2 = ACP^2 + AQP + F, \tag{4.7}$$

and the parameters AC, AQ and F, that are each dependent on the specific laser and measurement, can be experimentally characterised by measuring the voltage variance and performing a quadratic polynomial fit where with the optical power in the x-axis and the voltage variance in the y-axis. As mentioned above, the voltage noise intrinsic to the spontaneous emission is expressed by the parameter AQ in Eq. 4.7. Therefore, we define the Quantum-to-Classical Noise Ratio (QCNR) as

$$QCNR = \frac{AQP}{ACP^2 + F}. \tag{4.8}$$

The QCNR can be used to estimate the min-entropy generated and therefore it can be used to extract the amount of randomness produced, as shown in Section 4.5.

4.2 Description of the experimental setup

The schematic of our experiment is shown in Fig. 4.1. The light source was a Mitsubishi FU-68SDF-8 DFB laser diode (coherence time $\tau_{coh} \sim 2.5$ ns), driven by a Thorlabs CLD1015 module. It was followed by a polarisation controller to optimise the optical power injected into the chip, using vertical coupling with on-chip grating couplers with a 8-channel 127 μm VGA fibre array (OZ Optics). The chip used for this experiment was designed using the iSiPP25G technology and manifactured by IMEC[53][2]. Our SOI chip integrated a grating coupler to couple the light on chip, followed by a series of three Mach-Zehnder interferometers (MZI). Indeed, Eq. 4.2 is based on the assumption of perfectly balanced beam-splitter and lossless optical channel. When working in bulk and fibre optics these assumptions can be satisfied to a very high degree, due to the low losses in the optical fibres. However, fabrication errors in integrated SOI devices can alter the reflectivity. For example, the integrated multi-mode interferometers (MMIs) used in our experiment can have up to 0.5 dB excess loss. Moreover, the linear losses in the rib waveguide used as delay line are estimated to be around 1 dB/cm, which is not negligible in a long delay line. Therefore, in order to optimise the interference and phase noise to intensity noise conversion, our device was composed of a cascade of three MZIs where the input and output MZIs were balanced, (i.e. the length of the two arms is equal), and the relative phase between the two arms can be tuned by taking advantage of thermal phase-shifters. These acted as tunable beam-splitters. The central MZI was instead unbalanced, with a $T_d = 540$ ps delay line (4 cm), used to map the phase fluctuations of the electromagnetic field into intensity fluctuations. This central MZI had a thermal phase-shifter to configure the system to optimise the intensity fluctuations detected by the photodiodes. The light at the output of the MZI cascade was coupled into two integrated Ge photodiodes with a nominal efficiency $\eta = 0.8$ [53]. Two more grating couplers connected through a waveguide were used to monitor the optical coupling inside the chip. The photocurrent from the

[2]Further details about the technology used can be found in Section 3.11, as the experiment in Chapter 3 and this current chapter make use of the exact same SOI technology, provided by the IMEC foundry.

photodiodes was converted into a voltage signal by a custom made transimpedance amplifier (TIA). The output signal from the TIA was detected and digitalised by a fast GHz bandwidth oscilloscope DSO-V134A Agilent Keysight Technology and the data were further analysed by a desktop computer. The phase-shifters were digitally controlled by multi-channel heater drivers previously designed in our group (and in use in the last few years). In practise, the grating couplers, MZI and photodiodes occupied an area < 1 mm^2, integrated on a SOI chip with a footprint of 2.5 mm^2 that contained other optical designs. The chip was embedded and wirebonded to a 4×8 cm electronic printed circuit board, containing the TIA and the voltage supply for the photodiodes. This system was enclosed inside a Faraday cage, to reduce the RF environmental noise.

4.3 Characterisation of the MZIs series

As described by Eqs. 4.2 and 4.5, the maximum voltage fluctuations can be observed at $2m\pi + \pi/2$ in the unbalanced interferometer. In order to maximise the visibility of the output signal, particularly due to the losses in the integrated devices such as beam-splitter and waveguides, the input and output interferometers had to be carefully tuned. Therefore, we performed a scan of the phases for the three different phase-shifters to determine the configuration to maximise the visibility of the output voltage signal. In particular, for a given voltage applied to the ϕ_1 and ϕ_3 (as labelled in Fig. 4.1), ϕ_2 was varied in the range 0 to 2π, as reported in Fig. 4.2. From Fig. 4.2 it can be observed that varying the phases of the input and output interferometers, the visibilities vary, and the optimal value can be found where the visibility is maximised. The voltage to control the phase, shown in Fig. 4.2 was swept in steps of 0.2 V, from 4.0 V to 5.0 V for ϕ_1 (top to bottom in Fig. 4.2) and from 3.8 V to 4.4 V for ϕ_3 (left to right in Fig. 4.2). Moreover, for each combination of these phases, the voltage in the unbalanced MZI was scanned with a step of 0.03 V from 0 V to 3 V. The highest visibilities were obtained for values of respectively 4.8 V and 4.2 V.

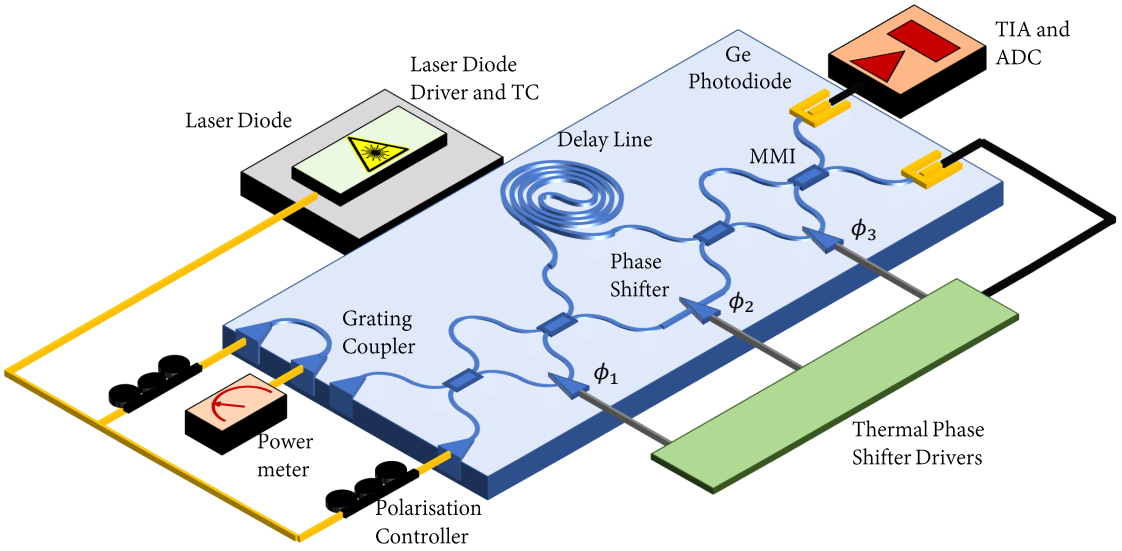

FIGURE 4.1: ***Setup for the experiment.*** *The light was generated by a laser diode, working at* $\lambda = 1540$ *nm, and injected via optical fibre into the chip through a V-groove array. In order to optimise the coupling, a polarisation controlled was used to tune the polarisation of the beam. The SOI chip was characterised by grating couplers for coupling the light, followed by a series of Mach-Zehnder interferometers. Each MZIs was composed of two ideally* 50% *multimode interferometers, acting as integrated beam splitters, and a phase-shifter, based on thermal heaters. While the input and output MZIs have balanced path lengths, the central MZI had a delay line on one arm, and it was therefore unbalanced. The device was designed with two Ge photodiodes at the outputs. These were used to detect the light intensity and convert it into current. On one output, a high speed transimpedance amplifier was used to convert the current into voltage, that will be analysed by a fast oscilloscope. On the other output, the signal was used to monitor the light intensity. This was useful to control and optimise the phase in the interferometers and maximise the phase noise fluctuations*[3].

4.4 Determination of the Quantum-to-Classical Noise Ratio QCNR

Any QRNG produces a signal where the desired *quantum signal* is mixed with a *classical noise*. This classical noise could be the background electronic noise of an amplifier, the electronic environmental noise due to the FM radio signal or to other

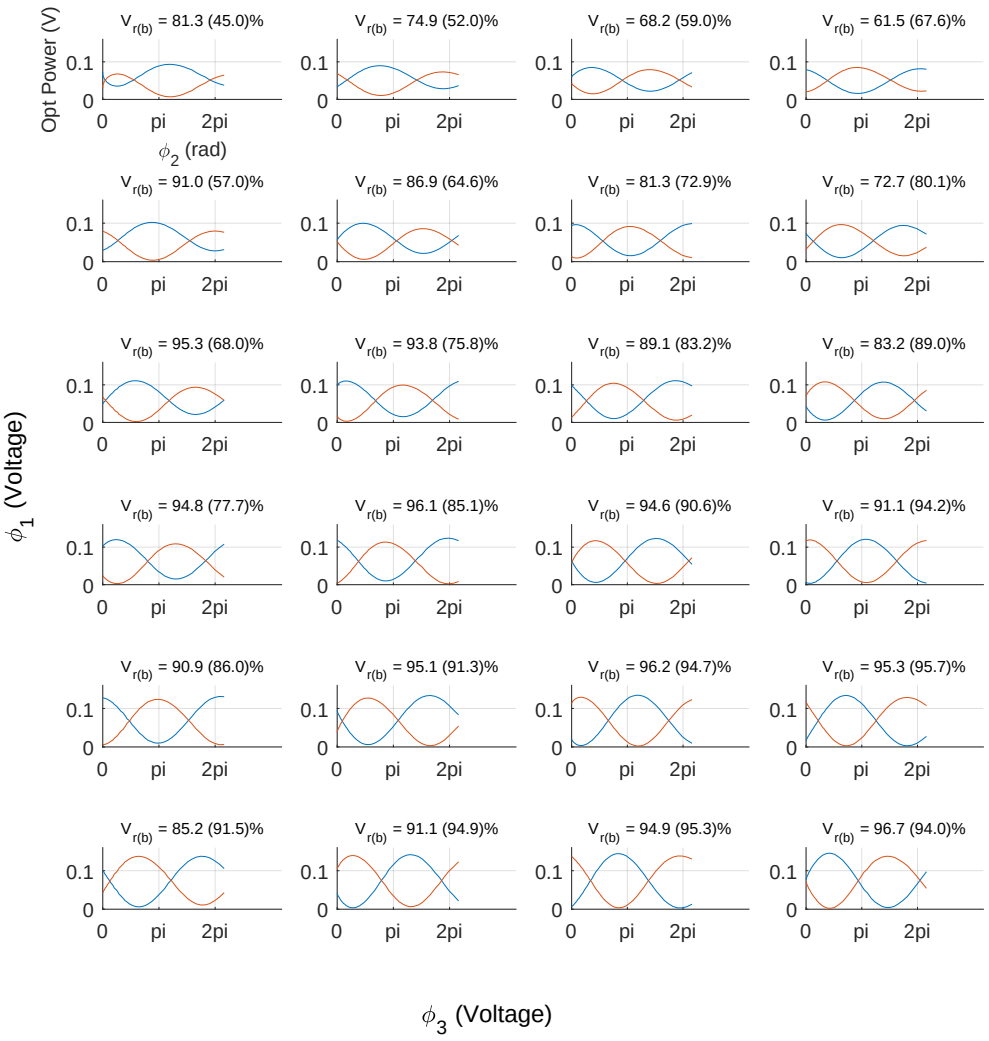

FIGURE 4.2: ***Voltage Fringes for the MZI cascade.*** *The fringes for different configurations of the phase in the MZIs are reported. Each row represents a different value in the phase of the input MZI (from 4.0 V for the top row to 5.0 V for the bottom row), whereas each column represents a different value of the output MZI (from 3.8 V for the first column to 4.4 V for the last column). In all the plots the phase of the unbalanced MZI is scanned, and the voltage at the output of the two photodiodes is plotted. The output for each plot is expressed in Volts, while the phase has been normalised and it is expressed in radians. The visibilities for the voltage fringes are reported for each configuration of the phase shifters.*

instruments. The classical noise could be also due to the laser source, when its behaviour is not ideal. This is the case of a QRNG based on phase noise from a diode laser. In fact, as explained in Section 4.1, the generation of random numbers is obtained by operating the laser near and above threshold where the spontaneous emission dominates the stimulated emission. However, the stimulated emission contribution is not completely eliminated, affecting the quality of the randomness produces. Hence, it is very important to be able to quantify the amount of quantum signal compared to the amount of classical signal in the measured sample. In this section we will report the method used to characterise quantum-to-classical noise ratio (QCNR), based on the theory described in Section 4.1.

4.4.1 Fringes of phase noise variance

The optimal conversion from phase fluctuations to intensity fluctuations is obtained where the interference fringes in the optical power present the maximum slope. This

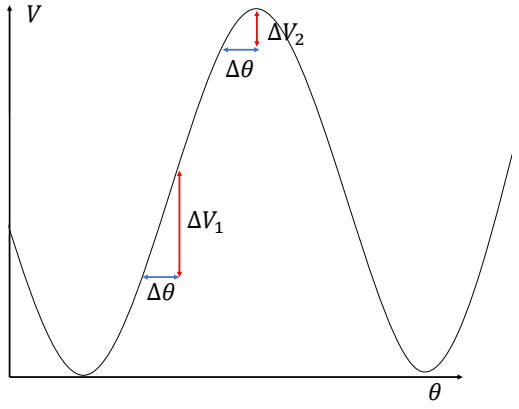

FIGURE 4.3: ***Relation between slope and phase noise variance.*** *Where the slope is maximum, a little change in the phase affects more the fringe value compared to phases characterised by a smaller slope.*

is due to the fact that, where the slope is maximum, a little variation in the phase has a bigger effect on the signal compared to where the slope is lower (see Fig. 4.3).

Moreover due to the fact that the laser diode wavelength changes with the input current, the fringes measured at each optical power will be shifted compared to

one another. As a consequence, the maximum in the phase noise variance will be observed at different voltages applied to the phase shifters in the unbalanced MZI. For this reason, in order to determine the QCNR, for each value of the input current the maximum phase noise variance must be extracted after scanning the phase of ϕ_2 inside a range of at least $(0, \pi]$. Hence, to characterise the phase noise variance as a function of the optical power, useful to extract the optimal QCNR, variance fringes at different power were measured, reported in Fig. 4.4[4].

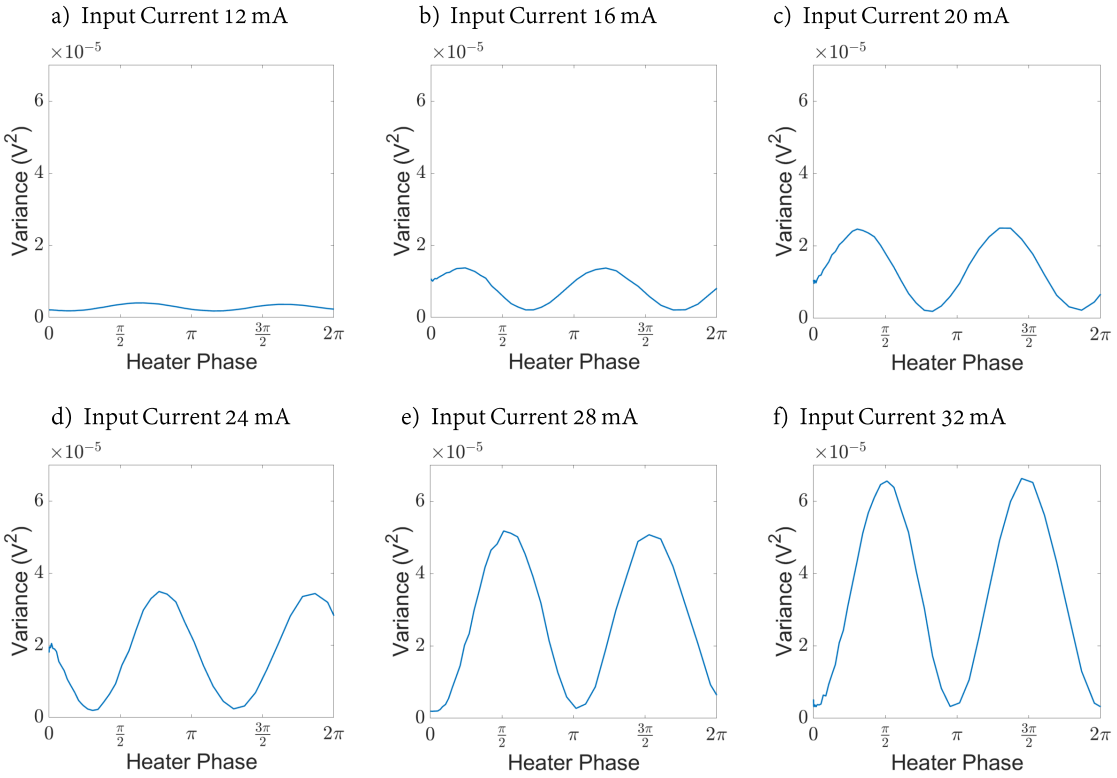

FIGURE 4.4: ***Measured fringes of the phase fluctuations noise.*** *Fringes of voltage variance at a few different values of the optical power injected into the SOI chip. By increasing the input current in the laser diode (and thus the optical power injected into the chip) the maximum voltage variance increases, in agreement with Eq. 4.7.*

From these fringes, by taking the maxima in the visibilities, it was possible to plot the variance of the phase fluctuations noise as a function of the optical power and consequently extract the QCNR, shown in Fig. 4.5. This enables us to subsequently

[4]Here just a few fringes are reported, to show the experimental procedure.

choose the best parameters to maximise the QCNR. Here it is important to notice that the quadratic fit and thus the QCNR is very sensitive to small changes in the measured variances. For this reason, it was important to properly weigh the least square algorithm used to extract the fit parameters. Otherwise, this would have resulted in the underestimation of the parameter F and AC and a consequent overestimation of the QCNR and hence a randomness overestimation. In particular, the value of the voltage variance corresponding to the optical power equal to zero was constrained to be very close to the electronic background. This operation was required to make sure that the fit would find the correct value for F in Eq. 4.7, in order not to overestimate the QCNR.

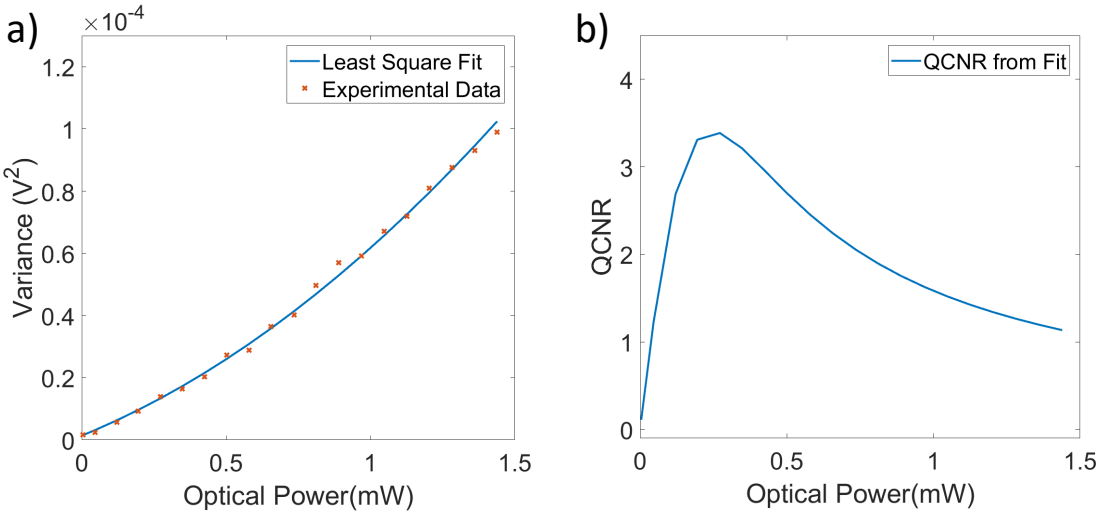

FIGURE 4.5: ***Phase fluctuations variance and QCNR as a function of the optical power.*** *a) Variance of the voltage noise for different values of the input current injected into the laser diode. A quadratic behaviour can be observed. b) QCNR at different values of the optical power, obtained from the quadratic fit, from Eq. 4.8.*

The parameter of the quadratic fit shown in Fig. 4.5, obtained from Eq. 4.7, are reported in Table 4.1.

Parameter	Value
$AC(\mathrm{V/W^2})$	22.519
$AQ(\mathrm{V/W})$	0.0378×10^{-2}
$F(\mathrm{V})$	1.3732×10^{-6}
R	0.999

TABLE 4.1: ***Statistical parameters of the least squares quadratic algorithm.*** *The parameters for the fit of the voltage noise variance as a function of the optical power as in Eq. 4.7 are reported.*

4.4.2 Experimental determination of the QCNR

Another experimental approach, not based on a quadratic fit, could be used to extract the QCNR. This second approach has the main advantage that the QCNR can be estimated experimentally for a single given value of the power, without requiring to estimate the variance due to the phase fluctuations at different powers. This second approach was also explained in Ref. [33]. The method lies on the fact that the phase fluctuations are due to a quantum contribution, that we called AQ and a classical contribution that we called AC. The quantum contribution will be dominant when the laser is operated just above threshold, while the classical contribution will be dominant when the laser diode is operated with a high input current. Hence, to estimate the QCNR we used the following procedure:

- Measure the variance σ^2 for a given power P_0;
- Measure the variance σ^2_{att} when the laser is operated at maximum input current, but the laser is followed by a optical attenuator such that the optical power is P_0;
- Calculate the ratio $\mathrm{QCNR}_{exp} = \frac{\sigma^2 - \sigma^2_{att}}{\sigma^2_{att}}$ which gives the estimate the ratio between the pure quantum contribution and the contribution due to the classical noise.

The experimentally measured QCNR is shown in Fig. 4.6. Here we can observe a good agreement between the QCNR obtained via quadratic fit and the QCNR

obtained experimentally with the method just described. It is worth noting here, that the maximum value for the QCNR and the optimal optical power, where the QCNR reaches its maximum value are consistent between the two methods. The discrepancy we observe between the two methods is probably due to the fact that, since the variable optical attenuator (VOA) had to be physically removed between the two set of measurements, this could have affected the polarisation of the optical beam and thus the optical power coupled on-chip.

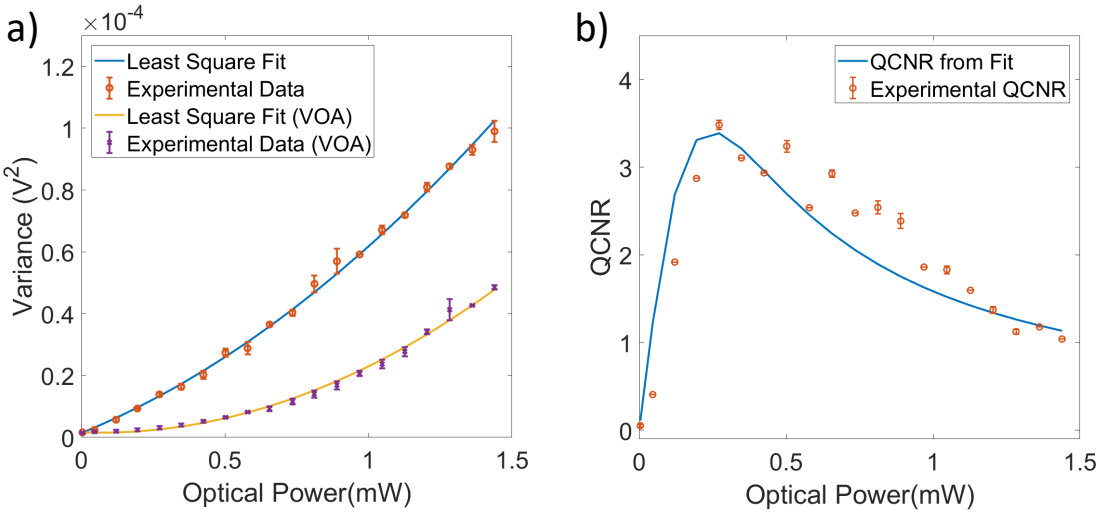

FIGURE 4.6: ***Experimental measurement of the QCNR.*** *a) The blue line is obtained by fitting the experimental voltage variance, directly measured by varying the input current into the laser diode, without VOA. The yellow line is obtained by fitting the experimental points when the VOA was introduced. In this second set of measurements, the input current injected into the laser is maximised, and the optical power is tuned by varying the attenuation at the variable optical attenuator. b) The orange points are obtained as the ratio between the experimental points in 4.6a. The blue line is obtained by fitting the blue line in 4.6a using Eq. 4.7.*

We remark here that during our experiment we used the method based on the quadratic fit to extract the QCNR. This was due to the limited power of the laser diode and the coupling losses of the VOA used. Indeed to obtain the plot in Fig. 4.6, the VOA had to be physically removed to obtain σ^2. Ideally, with a VOA with lower coupling losses, it would be possible to estimate the maximum QCNR without the

need of measuring the fringes for different values of the optical power. This method would be more time efficient compared to the method based on the polynomial fit.

4.5 Estimation of the min-entropy H_∞

Similarly to Chapter 3, in order to estimate the maximum extractable randomness the min-entropy of the digitalised voltage signal could be calculated. The expression

$$\mathrm{H}_\infty = -\log_2(\max_{x\in\{0,1\}^n} \Pr[X = x]) \tag{4.9}$$

is the min-entropy, where n is the number of bits used in the digitalisation of the voltage signal and $\Pr[X = x]$ is the probability of the voltage measurement x, falling in the X bin.

It is important here to recall that Eq. 4.9 is valid only the assumptions described in Section 2.4.2.1 and summarised below [65]:

- The quantum and classical signals are independent.
- The total variance σ^2 can be determined by sampling the raw signal. This implies that the samples are independent and identically distributed (iid).
- $\Pr[X = x]$ being the distribution of the quantum signal is known or can be determined.

Here we will explain the procedure used to extract the min-entropy. We mentioned that one of the conditions to use Eq. 4.9 is that the probability distribution of the quantum signal $\Pr[X = x]$ can be determined from the measured distribution which contains the quantum signal as well as the classical noise. In this case, this assumption is valid given that all the contributions to Eq. 4.7 are described by a Gaussian distribution. In fact, the quantum phase noise Q, being produced by a large number of independent noise events due to spontaneous emission, has a

Gaussian distribution described by

$$p(\Delta\phi) = \frac{1}{\sqrt{2\pi\langle\Delta\phi^2\rangle}} e^{-\frac{\Delta\phi^2}{2\langle\Delta\phi^2\rangle}},$$

where ϕ is the phase [99]. As described in [101] the classical phase noise contribution C is due to carriers oscillating between valence and conduction bands, due to thermal effect. As a consequence, also the term C in Eq. 4.7 is characterised by a Gaussian distribution. Finally, the electronic noise has different contributions, where the thermal and shot-noise, characterised by Gaussian distribution dominate for wide bandwidths, validating the assumption of Gaussian electronic noise. $\Delta V(t)$ has a Gaussian distribution, being the linear combination of three different Gaussian contributions. For this reason, the voltage variance due to the quantum phase fluctuations is obtained as

$$\sigma_q^2 = \frac{\sigma^2}{1 + \frac{1}{QCNR}}. \tag{4.10}$$

The following procedure was applied to our experiment to determine the min-entropy:

- For different values of the optical power, we swept the phase of the central interferometer from 0 to π, recording the fringes of the variance as in Fig. 4.4.
- For each optical power, we selected the maximum variance from the fringe.
- We plotted the maximum variance as a function of the optical power, and extracted the QCNR by using Eq. 4.8;
- We calculated σ_q^2;
- We chose a voltage range in the oscilloscope to optimise the information contained in the measured signal (for example $V(max, min) = \pm 5\sigma$);
- We divided the interval into 2^{n} bins, where n is the number of bits used in the digitalisation;
- We thus integrated the signal over the bins and normalise the distribution to obtain $Pr[x]$ as in Eq. 4.9;

- Finally we calculated the min-entropy H_∞.

The oscilloscope used for this experiment was a DSO-V134A from Agilent Keysight Technology, with a sampling resolution of 8 bits. As shown in the previous paragraphs, we obtained QCNR ~ 3.4. This value was obtained with an input optical power into the chip of $P_{in} = 300$ μW. From Fig. 4.5 we can see that the variance measured by the oscilloscope is $\sigma^2 = 1.33 \times 10^{-5}$ V^2. Therefore we selected a voltage range $V(max, min) = \pm$ 15 mV and divided it into 256 equally spaced bins. Finally, we estimated the min-entropy to be $H_\infty \sim 5.6$ bits/sample. Here we notice that this derivation was done under the assumption that $\Delta V(t)$ followed a Gaussian distribution. The assumption of Gaussian noise is confirmed by Fig. 4.7 where we can observe a good agreement between the experimental data and the Gaussian fit. A minimal skewness can be observed in the experimental histogram of Fig. 4.7. This is due to a imperfect shielding of the experimental setup from the environmental FM noise and to the imperfect electronics. However, the agreement between the experimental data and a Gaussian curve, as well as the skewness of the data, has been quantified and the results are reported in Table 4.2. The parameter R for the Gaussian fit is above 0.99 confirming a very good agreement between the fit and the experimental data. The skewness has been measured to be -0.1773. Usually, when between $\pm$ 2, the skewness is considered acceptable to prove a Gaussian distribution [102].

Parameter	Value
A	2314
B	35
C	12.24
R	0.992
skewness	-0.1773

TABLE 4.2: ***Statistical parameters of the least squares quadratic algorithm.*** *The parameters for the Gaussian fit are reported, where the equation considered was* $f = A\exp\left[\frac{x-B}{C}\right]^2$.

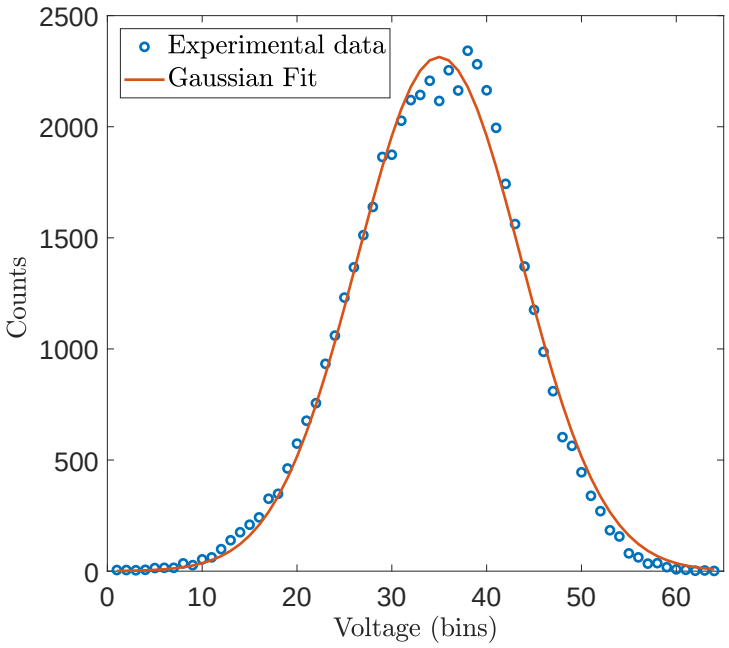

FIGURE 4.7: ***Histogram of the raw samples.*** *In this figure we report the histogram of the raw samples measured by the oscilloscope. It can be observed that they are normally distributed. This is necessary condition to extract the min-entropy using the method described in this section.*

4.6 Bandwidth and generation rate estimation

To determine the optimal sampling rate of the device, the spectral density of our QRNG was measured in absence and presence of the optical signal. The result is reported in Fig. 4.8. Here we observe that the optical signal is above the electronic noise up to approximately 500 MHz. From Fig. 4.8 we can also observe some peaks, mainly around 100 MHz, which is the environmental noise arising from background radio frequencies. However, the signal is roughly 10 dB above the noise floor, so the environmental noise does not influence the generation of random bits. Taking into account a sampling rate of 500 Msamples, and a min-entropy $H_\infty = 5.6$ bits/sample when sampling at 8 bits/sample, we estimated a randomness generation rate of nearly 2.8 Gbps.

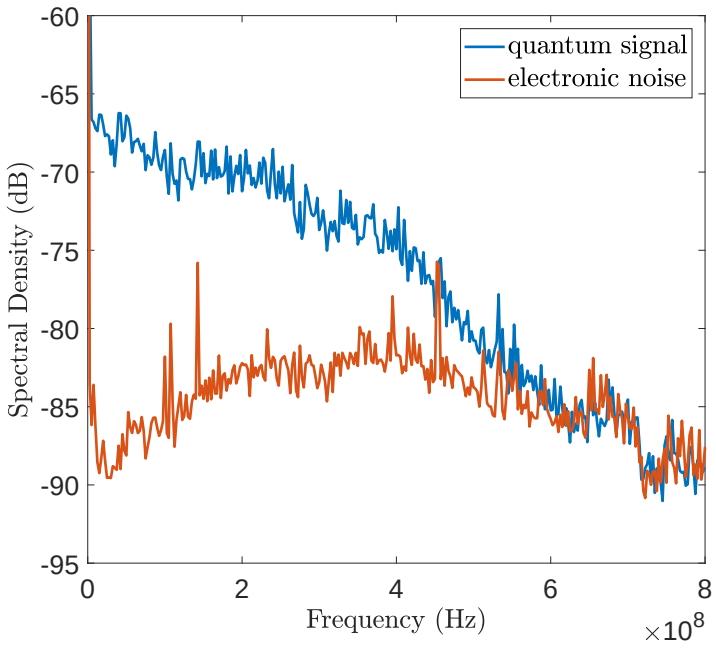

FIGURE 4.8: ***Spectral density for quantum signal and noise floor.*** *The spectral density for the optical signal and for the electronic noise floor are reported. It can be observed that the quantum signal is above the electronic noise up to 500 MHz. The noise floor presents some peaks due to environmental noise, particularly around 100 MHz. These are FM radio signals, which however are below the quantum signal and therefore are not affecting the quality of the generated random numbers.*

4.7 Autocorrelation of the bit samples

A first estimation of the quality of the bit sequences is given by the autocorrelations of the samples, defined in Section 3.7. In fact, environmental RF noise, oscillations in the transimpedance amplifier and oversampling are the main cause of periodic oscillations in the signal that can result in correlated bit sequences. Moreover, these factors could be in principle controlled classically by an adversary. For this reason we measured the autocorrelation of the signal, acquired at different sampling rates. As expected, the optimal sampling rate appears to be 500 Msamples/s. This is because of the spectral density of the detector, where the optical signal is well above the electronic noise up to 500 MHz. On the other hand, oversampling at 5 Gsamples/s results in highly correlated sequences, as shown by the yellow line in Fig. 4.9a.

It can be observed that correlations up to around 5% can be observed in the raw signals within a few samples also for the 500 Msamples line. This might be due to due finite bandwidth of the transimpedance amplifier, and to the residual classical noise affecting the signal. In agreement with the assumptions made for the min-entropy calculations, we considered this residual correlations as part of the classical contribution to the signal. As it can be observed by Fig. 4.9b, the hashed signal does not present any correlation.

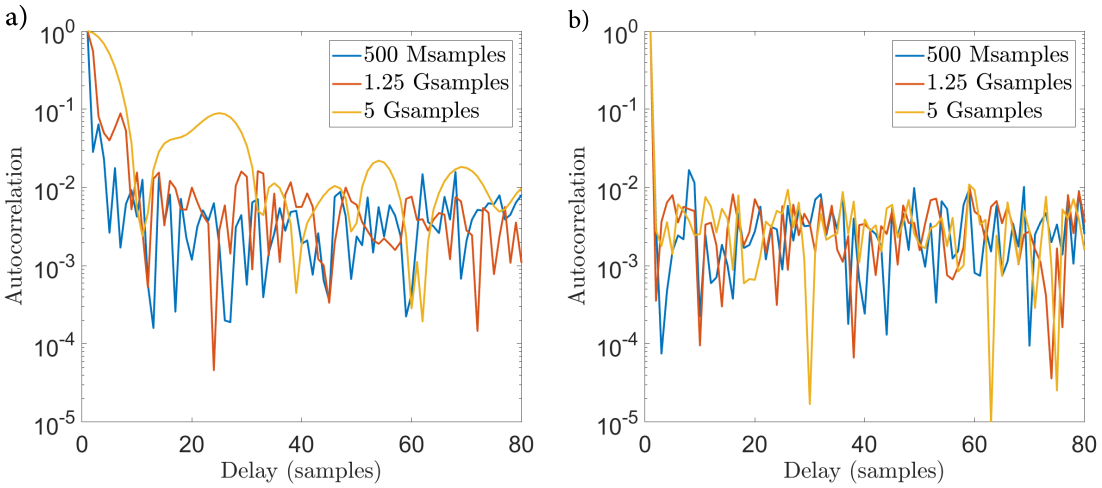

FIGURE 4.9: ***Autocorrelation of raw and hashed bits.*** *a) We report the autocorrelations of the raw signal, obtained after digitizing the signal, for different sampling rates. We notice that for sampling speeds above the bandwidth the autocorrelations can be up to one order of magnitude bigger than the when sampling at 500 Msamples. b) The hashing reduces drastically the autocorrelations. No appreciable difference can be observed in this case between different sampling speeds.*

4.8 NIST statistical test

In this section we report the results of the statistical tests on our QRNG provided by the National Institute of Standards and Technology (NIST SP 800-22). More explanation on the suite of tests used can be found in Sections 3.8 and 2.4.3. Here we remark that the raw bit extracted had been post-processed following the procedure reported in [65] and briefly described in Sections 2.4.2.2 and 3.6.

NIST SP800-22		
Test name	Pass Rate	P-value
Frequency	0.989	0.891
Block Frequency	0.993	0.128
Cumulative Sums	0.987	0.186
Runs	0.989	0.177
Longest Run	0.992	0.768
Rank	0.995	0.360
FFT	0.984	0.465
Non Overlapping Template	0.995	0.014
Overlapping Template	0.986	0.155
Universal	0.985	0.800
Approximate Entropy	0.984	0.573
Random Excursions	0.993	0.115
Random Excursions Variant	0.989	0.011
Serial	0.991	0.169
Linear Complexity	0.993	0.768

TABLE 4.3: ***Statistical tests on the random data.*** *The results for the NIST (National Institute of Standards & Technology) statistical tests suite [93]. In order to pass the NIST SP800-22 the pass rate must be above 0.98 for each type of test (column II) and the reported P-values, which refer to the uniformity test on the distributions plotted in Fig. 4.10, must be above 0.01 (column III).*

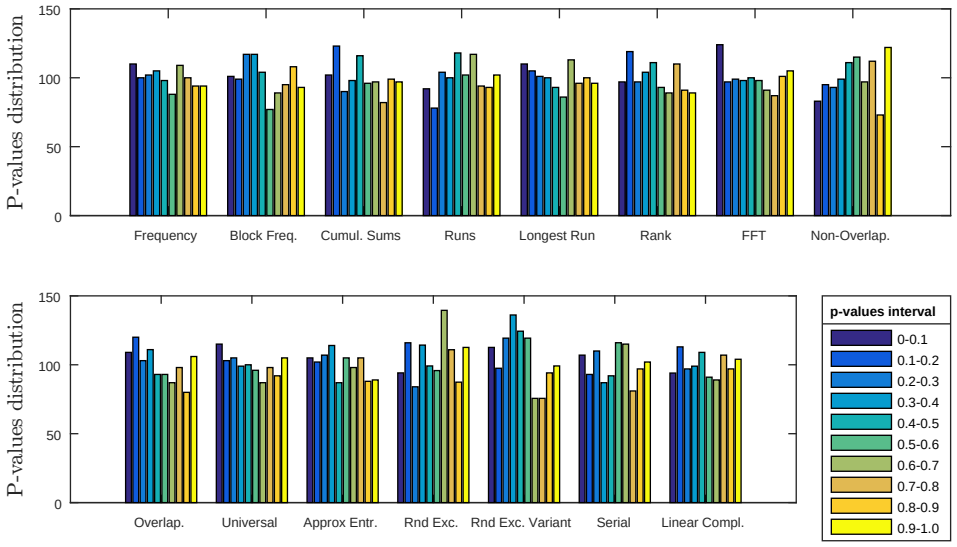

FIGURE 4.10: **Uniformity test for the P-values.** Under the assumption that the produced random bits are truly random, the P-values must be uniformly distributed between 0 and 1. Here the NIST statistical test provides the frequencies of the P-values, by dividing the (0,1) interval into 10 sub-intervals. We can observe that for each test the P-values are uniformly distributed.

4.9 Stability

Among the main advantages of working with integrated photonics are the compactness and monolithic nature of the devices. While compactness enables the parallelization of multiple components into a single microchip, the monolithic nature has the main advantage of eliminating almost completely many forms of instability. This is particularly useful when dealing with interferometry and unbalanced interferometers. When working with optical fibres, small changes in temperature can affect the length of the fibre enough to destroy interference. In free-space instead, the stability is threatened by any environmental factor that generates oscillations in the optics. By reducing the size of the systems, and by integrating everything in a single chip, these issues are drastically reduced. This fact was particularly relevant in our experiment. In fact, as it can be observed in the red line of Fig. 4.11, the system was perfectly stable in a time range of around one hour. This stability was reached by simply calibrating the phase of the unbalanced interferometer every 2-3 minutes. This was obtained by interrupting the signal acquisition and sweeping ϕ_2 in phase interval $(0,\pi]$ in order to select the value of ϕ_2 that maximised the variance of the voltage noise. In fact this could have slightly shifted due to temperature changes in the chip. Once the optimal phase was found the acquisition could start again. This method proved to be robust in the time scale of at least one hour. Moreover, even without any calibration in the phase of the interferometer, the variance of the signal (blue line), was stable over a time interval of several minutes. Here it is important to mention that only the voltage in the unbalanced interferometer was scanned, while ϕ_1 and ϕ_3 remained untouched after a preliminary characterisation.

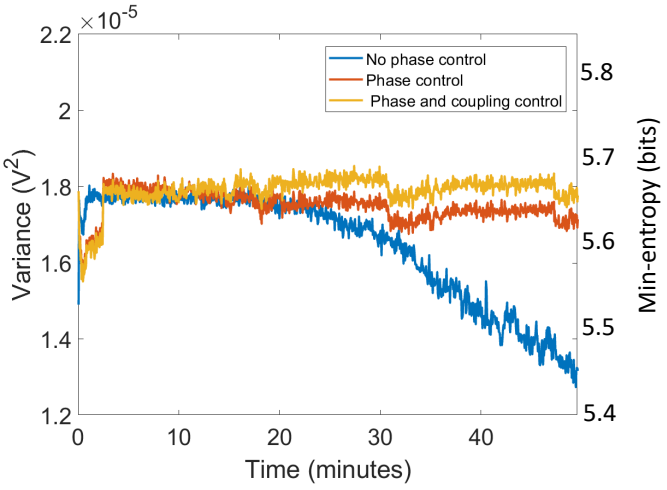

FIGURE 4.11: ***Signal variance measured over a time interval of one hour.*** *The variance of the signal measured by the oscilloscope was measured over a time interval of 50 minutes. The blue line shows the behaviour of the variance without any control on the phase of the integrated MZIs. The red line shows the variance when the phase of the unbalanced MZI have been calibrated every 2 minutes. The yellow line has been obtained by normalising the variance plotted in red with the optical power coupled into the chip. It can be seen that, beside some variation due to the change in the fibre-chip coupling, a phase calibration every few minutes is sufficient to keep the system perfectly balanced.*

4.10 Discussion

In this chapter we demonstrated in a highly compact footprint, the integration on a monolithic silicon-on-insulator chip of all the photonics needed for the readout of QRNG based on phase fluctuations from an external laser diode. Our scheme shows good stability and low optical power operation combined with Gbps generation rate.

By comparing our results with those reported in [34], we see that they strongly outperform our device in terms of generation rates. This is due to different reasons. On one hand, they generate the random numbers at an optimal optical power of approximate 1 mW, while the optical power injected in our silicon chip is 300 μW, with an estimated optical power at the photodiodes of 40-50 μW, due to the linear losses that occur in the waveguides and in the integrated MMIs. Hence a difference of a

factor 20 between our demonstration and [34] is a first motivation that partially explains the difference in generation rate. A second cause is the different method used to sample the analog signal, which is then converted into the bit-string. Indeed, we limited our sampling rate to be comparable to the bandwidth of our transimpedance amplifier. This choice was due to the fact that by oversampling we would introduce correlations in the raw bit-string. In [34], the author sampled the analog signal beyond the physical bandwidth of the TIA, assuming that any classical correlation would then be erased by the randomness extraction, namely the Toeplitz algorithm. While their assumption might provide a hashed bit-string, it is not clear whether by sampling far beyond the physical bandwidth of the quantum signal it is still possible to describe this as a quantum random number generator or rather a fast true random number generator, where the classical noise, instead of being quantified and removed from the signal, contributes to the random signal as electronic noise.

There are a few possible ways to further improve the generation rates. An immediate enhancement in the generation rate could be achieved with a more powerful laser source. However, as previously mentioned, this could be detrimental for the stability of the device and whenever the QRNG needs to be integrated within a dense, complex chip. Higher optical power in the delay line would be likely to induce heating in the waveguide and therefore changes in the path length of the signal. This would probably reduce the phase stability of the system. Given the high reproducibility of this SOI photonic device, another option could be to substitute the input and output MZIs with simple MMIs. Considering the quoted losses at each MMI of roughly 0.5 dB, the total gain in terms of optical power detected by the photodiodes could be up to 20%. While the input and output MZIs were very useful at the characterisation stage, they remained untouched during the random bit generation. A higher optical signal at the photodiodes would also relax the need for low-noise transimpedance amplifiers (TIA), allowing the use of faster TIAs.

Besides, a qualitative analysis of the parameters involved in this experiment shows how these could be optimised to increase the generation rate by orders of magnitude. The length of the delay line in the interferometer is constrained by the coherence

length of the laser, as T_d must be smaller, but possibly close to τ_{coh}. The bandwidth defines an upper bound for the sampling rate. The inverse of the sampling rate must be greater than the time delay occurred in the delay line. Hence, given the vast choice in the linewidth and optical power of laser diodes, the ultimate speed of this kind of QRNG is limited by the bandwidth of a TIA and enhancing the bandwidth would have multiple advantages. As just explained, a higher bandwidth would enable higher sampling rates, which is a primary advantage. Although, a higher sampling rate would require a reduction in the length of a delay line, which brings further advantages. A shorter delay line would reduce the linear losses and therefore increase the optical power at the photodiodes. Moreover a shorter delay line would reduce the phase instabilities that occur inside the waveguides. In addition, a short delay line would reduce the footprint of the device. Finally, this protocol, specifically in its integrated version, shows potential for improvements.

More research should be done also in the choice of the TIA. Faster TIAs not based on operational amplifiers with comparable noise level and bandwidths beyond 1 GHz are available. In Chapter 6 a more detailed analysis of possible solutions for faster TIAs can be found.

Looking at the compactness of the device, here the laser diode was external and vertically coupled to the chip by using a V-groove array. In order to further reduce the size of the system and to make the scheme more scalable, a heterogeneous integration can be envisaged, as shown, for example in [103], where a VCSEL laser is directly coupled to a Silicon waveguide through a flip-chip technique.

A final note related to this kind of QRNG is to what extent this can be considered a quantum random number generator. As shown in Sec. 4.11, spontaneous emission is a purely quantum effect that cannot be explained with a classical or semi-classical physical model. Spontaneous emission is present only if both the EM field and the atom are both treated as quantum mechanical systems. Therefore, even though the overall random phase appears as a random walk and therefore one might assume a classical description of the process, the single spontaneous event which contributes to the total random phase cannot be reduced to a classical phenomenon, and on

this fact is based the claim that this kind of a random number generator is indeed a quantum random number generator. Furthermore, the phase noise due to spontaneous emission can be isolated from the phase noise due to classical effects [101] (as we did in this chapter, following [33, 34]), and therefore the randomness of quantum origin can be estimated to a high degree of confidence. Ultimately, it is the possibility of estimating the quantum contribution, isolating it from the classical noise, that enables us to consider this as a QRNG. Nonetheless, given the higher level of guarantee, one might prefer the homodyne detection based QRNG of Chapter 3 when higher levels of security are required.

4.11 Appendix A

4.11.1 Phase noise in semiconductor lasers

Here we report a derivation of Eq. 4.6, obtained in Ref. [100]. The change in the amplitude of the electromagnetic field due to a spontaneous emission event can be written as

$$\Delta E_i = e^{i(\phi+\theta_i)}, \tag{4.11}$$

where, as shown in Fig. 4.12, ϕ is the initial phase and θ_i is the phase added by the spontaneous event. The validity of this equation is confirmed by the fact that, taking it into account, the intensity of the electromagnetic field is changed by the correct amount (more details can be found in [100]). The phase change due to the spontaneous emission can be divided then into two contributions, that we call $\Delta\phi_i'$ and $\Delta\phi_i''$. $\Delta\phi_i'$ is obtained directly by the change in phase due to a spontaneous emission event, and, from Fig. 4.12, it can be observed to be such that

$$\Delta\phi_i' = \frac{1}{\sqrt{I}} \sin\theta_i. \tag{4.12}$$

The amplitude due to this event changes as

$$\Delta I_i = 1 + 2\sqrt{I}\cos\theta_i, \tag{4.13}$$

where for the last equation the law of cosines has been applied. Given that for random events θ_i has a Gaussian distribution between 0 and 2π, $\cos\theta_i$ averages to zero, each spontaneous emission should contribute by adding one photon per mode. However, given the very high number of photons involved, the intensity fluctuations due to interference are comparable to a change of hundreds of photons. In order to derive the change in phase due to the intensity change, we consider the rate equations for light intensity and phase [100].

$$\dot{\phi} = \frac{\alpha}{2}(G-\gamma) \tag{4.14}$$

$$\dot{I} = (G-\gamma)I. \tag{4.15}$$

Combining the two equations under the assumption of a slowly varying intensity, and after integration, $\Delta\phi_i''$ can be written as

$$\Delta\phi_i'' = -\frac{\alpha}{2I}\Delta_i = -\frac{\alpha}{2I}(1 + 2\sqrt{I}\cos\theta_i). \tag{4.16}$$

Summing the two contributions to the phase change we obtain

$$\Delta\phi_i = \Delta\phi_i' + \Delta\phi_i'' = -\frac{\alpha}{2I} + \frac{1}{\sqrt{I}}\left[\sin\theta_i - \alpha\cos\theta_i\right]. \tag{4.17}$$

From this, calculating the variance of the phase change $\Delta\phi$, due to many spontaneous emission events, we obtain, for an integration time t and a spontaneous emission rate R,

$$\langle\Delta\phi^2\rangle = \frac{R(1+\alpha^2)t}{2I}. \tag{4.18}$$

Here we can observe the inverse relation between the variance in the phase fluctuations, as a function of the intensity, and thus of the optical power, as expressed

in Eq. 4.6. However, in Eq. 4.18, the classical term, independent of the intensity, is not present and thus Eq. 4.18 can be considered only valid for values close to threshold. The intensity independent term is due to the fluctuations of the state occupancy in the conduction and valence bands, caused by intraband thermalization processes. This effect was studied in more detail in [101] and it will not be reported here.

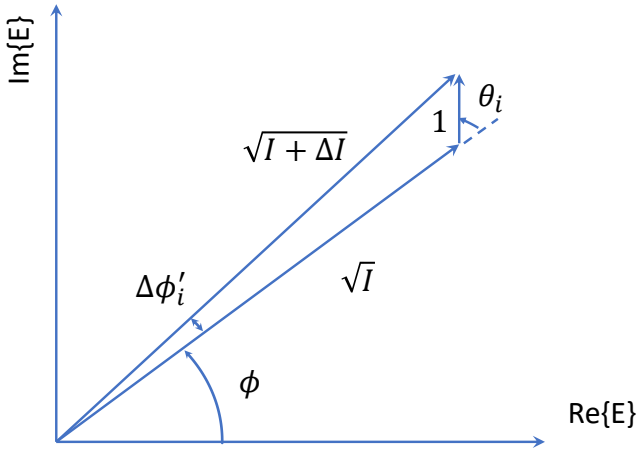

FIGURE 4.12: ***Representation of phase change.*** *In this example the field amplitude $\sqrt{I}$ is increased to $\sqrt{I+\Delta I}$ as a consequence of an instantaneous phase change, due to spontaneous emission.*

4.11.2 Quantum Nature of Spontaneous Emission

QRNGs based on phase fluctuations from laser diode exploit the phenomenon of spontaneous emission. Spontaneous emission is a purely quantum effect, that cannot be explained without Quantum Mechanics. Specifically, when considering a system composed of an atom interacting with an electromagnetic field, both the atom and the field must be described by a quantum mechanical model. Otherwise, considering a classical electromagnetic field, the spontaneous emission cannot be explained [104].

It can be shown that for a classical electromagnetic field, described by $\mathbf{E}(t) = \mathbf{E}_0 \cos \omega t$, interacting with an atom, the probability of transition from an initial

state $|i\rangle$, to a final state $|f\rangle$ is

$$P_{i\to f}^{(I)}(t) \propto \frac{|(\hat{\mathbf{d}} \cdot \mathbf{E_0})_{fi}|^2}{\hbar^2}. \tag{4.19}$$

Thus, the probability of transition between two states goes to zero for $\mathbf{E_0} = 0$ and hence the phenomenon of spontaneous emission is not predicted when a model with a classical electromagnetic field is considered.

On the other hand, by considering a quantized electromagnetic field, the matrix element describing spontaneous emission, i.e. describing the system passing from a quantum system described by $|a\rangle|n\rangle$ to $|b\rangle|n+1\rangle$, where $|a\rangle$ and $|b\rangle$ are the inital and final state of the atom n is the number of free photons is

$$\begin{aligned} \langle f|\hat{H}^{(I)}|i\rangle &= \langle b, n+1|\hat{H}^{(I)}|a, n\rangle \\ &= (\hat{\mathbf{d}} \cdot \epsilon_{\mathbf{0}})_{ba}\sqrt{n+1}. \end{aligned} \tag{4.20}$$

It can be observed here that the matrix element is not zero, even for an initial state with $n = 0$ (more details in Chapter 4 of [104]). Here $\hat{\mathbf{d}} \cdot \epsilon_{\mathbf{0}}$ is non null for an atom where the energy levels described respectively by $|a\rangle$ and $|b\rangle$ are such that the number of electrons in the state a is greater than zero, which is the condition for spontaneous emission. Ultimately, the impossibility of a classical description of spontaneous emission is the justification for a QRNG based on phase fluctuations from a laser diode.

Chapter 5

Indium Phosphide fully integrated QRNG based on coherent light

In this chapter we report the studies and results in respect of a fully integrated Indium Phosphide (InP) QRNG based on measurements of coherent light. This is intended to improve the level of integration beyond that of Chapter 3 by integrating the laser diode and photodetection onto the same InP chip. Due to technical issues and time limitations, the initial plans were modified and the experiment was not completed as intended. However, the reported results show the feasibility of the technology and help define the steps required to bring it to completion. Philip Sibson designed the InP photonic chip and I performed the reported experiment. I was responsible for characterising the photonic chip and designing and testing the electronics. Jonathan Matthews supervised throughout the experiment and Jake Kennard contributed with helpful discussions.

5.1 Introduction

Since their first demonstration, QRNGs based on homodyne detection [24] have been realised in different situations, with different experimental setups, different generation rates and different approaches for the data post-processing [25–30, 40],

as reviewed in Chapter 3. However, all these demonstrations were built either in fibre optics or with free space components, making them impractical and making any potential large scale deployment extremely expensive. In order to limit the issues caused by the adoption of bulk optics, in Chapter 3 we reported the implementation of a QRNG based on homodyne detection where the homodyne detector, which included an integrated MMI and two Germanium photodiodes, was integrated on a Silicon-on-insulator chip. While the results reported in Chapter 3 are good both in terms of signal-to-noise ratio and randomness generation rates, an SOI demonstration of homodyne detection still required an external laser source, adding complexity to the system[1].

Potential improvements can be found by taking advantage of the Indium Phosphide (InP) photonic platform, where all the basic optical and opto-electronic components, including the laser diode, can be monolithically integrated on a single device of a comparable size to the SOI chip demonstrated in Chapter 3 and 4. After a great development of classical InP integrated photonics [56], InP has started finding applications in Quantum Key Distribution [105] and as a platform for QRNGs [41][2]. In particular, a high-rate QRNG fully integrated on an InP chip has been already demonstrated [41]. In that instance an integrated laser diode was modulated at high speed to produce independent pulses with a random phase relation between two consecutive pulses. The pulses were interfered with a second integrated laser diode operated in continuous wave mode and the interference between these two beams produced a signal with random amplitude. This signal was measured by an integrated photodiode and the photocurrent was digitalised. Because of the intrinsic random amplitude of the measured signal, this could be used to produce random numbers.

While such an InP fully integrated QRNG shows good performance both in terms of compactness and generation rates, a QRNG based on shot-noise measurements

[1]Here we note that also the experiment reported in Chapter 4 does not integrate the laser diode in the SOI chip.

[2]See also [56] for a review about the InP technology.

from a laser diode could potentially provide a few advantages. For example, source-device independent QRNGs based on homodyne measurements have been recently demonstrated with off-the-shelf fibre optics [28–30] and this could be directly applied to our experiment. Such a scheme would provide a stronger guarantee on the generated random bits. Specifically, in [28–30] the source can be left *untrusted*, and the security of the system can be certified by performing specific quadrature measurements on the vacuum states. This attribute makes these schemes more appealing for real-world applications, since the device will be protected from certain potential attacks. Moreover, homodyne detection schemes do not require high-speed modulation of the laser diode source, and have lower requirements in terms of phase stability compared to schemes such as those reported in [41] or even in Chapter 4. Therefore, generation of random numbers based on homodyne measurements is less demanding in the respect of hardware, and yet the achievable generation rates are still comparable to schemes such those reported in [41].

5.2 Experimental Setup

The main motivation of this experiment is the possibility of performing homodyne detection measurement in a device that is millimetre scale, where laser source and homodyne detector are monolithically integrated onto the same chip. A secondary motivation is to provide the first step for performing on-chip homodyne tomography for quantum optics on InP [106–108]. From the perspective of using the homodyne detector as a QRNG, this has the advantage compared to Chapter 3 that the laser is integrated and therefore all the photonic components of the QRNG are contained in a single chip, without the need of external light sources and without the need for coupling the light on-chip.

In Fig. 5.1 and 5.2 respectively we illustrate the InP photonic chip and the scheme of our experimental setup. Our InP chip was fabricated by outsourcing to the Oclaro foundry, as part of a multi-project wafer. The laser source was composed of a semiconductor optical amplifier region (SOA) delimited by two tunable distributed

Bragg reflectors (TBR) (see relevant section in Chapter 2) and it was controlled by an Arroyo Instruments Laser Diode Controller 6301. The MZI was composed of two MMIs and a thermal phase-shifter, driven by a desktop computer. For characterisation purposes, one of the optical outputs could be coupled off-chip to optical fibres using edge coupling to measure the optical power produced by the integrated laser, while the other output was coupled directly into an integrated homodyne detector (IHD). The IHD was characterised by a 50% MMI, where the outputs were coupled into two integrated photodiodes. The photocurrent from the photodiodes was amplified and converted into voltage by a transimpedance amplification stage. The voltage analog signal could be analysed by a fast oscilloscope from Keysight Agilent Technology (DSOV134A) or an electronic spectrum analyser. The InP chip was temperature stabilized using a temperature controller from Arroyo Instruments.

5.3 Prologue: breaking one photodiode and working without it

The reported results are affected by some issues encountered at the initial stages of the experiment:

- The photodiodes were subject to the wrong bias voltage (positive voltage bias). This was due to a mis-understanding of the specifications provided by the foundry. The major consequence of the direct bias was that one of the two photodiodes was irreversibly damaged such that it does not function. Therefore the subsequent characterisation was performed on the only remaining functional photodiode. The choice of proceeding with a single photodiode (instead of taking a new chip) was due to the limited number of copies of this chip available for this experiment and the limited remaining experimental time for my PhD studies. This choice is justified later in this section.

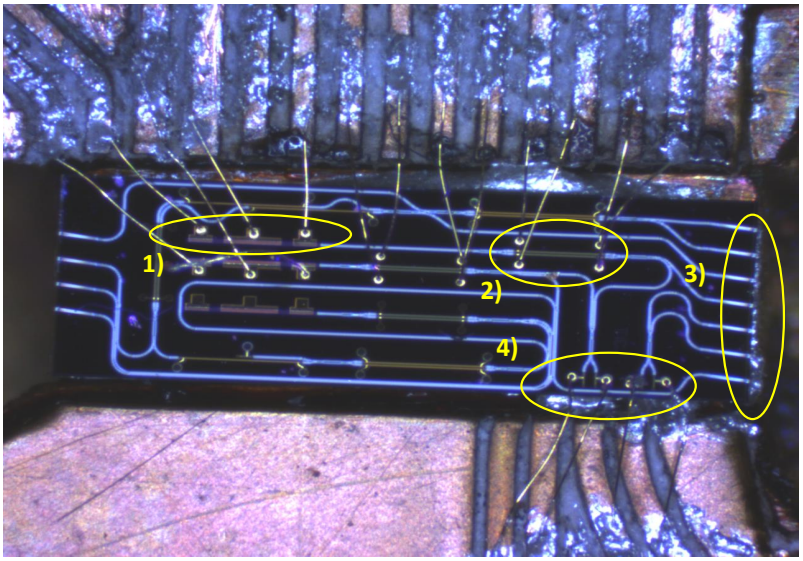

FIGURE 5.1: ***InP fully integrated homodyne Detector.*** *Image of the InP chip. The chip size is around 2 mm × 6 mm and is glued onto an electronic printed circuit board. The chip is electrically controlled through the wirebondings that can be observed in the picture. 1) Integrated DBR laser: the central wirebond is used to inject the input current into the SOA of the laser while the other wirebonds are used to tune the tunable Bragg grating used to tune the wavelength. 2) Integrated MZI with two phase-shifters used to control the optical power injected into the photodiodes. 3) Edge couplers used to measure the optical power from the integrated laser diode. 4) Integrated photodiodes with the floating anode that is wirebonded to the printed circuit board. NOTE: the size of the experiment is approximately half of the chip used, which also contains designs for other experiments.*

- Given the specific design of the integrated photodiodes, the readout electronics required the testing of different solutions compared to the schemes used in Chapter 3 and 4. These are briefly introduced in Sections 5.5.1 and 5.5.2 and further details can be found in Chapter 6.

- In an attempt to increase the performance of the electronics (while keeping the costs low), the choice of the material for the printed circuit board for the InP brought many limitations. Above all, the phase-shifter used to tune the optical power into the photodiodes did not work probably due to faulty wire-bonds

between the photonic chip and electronic printed circuit board[3].

In Fig. 5.2a we illustrate the ideal scheme of the device and in Fig. 5.2b we show the device as we used it in this experiment. All the results reported in the following sections refer to Fig. 5.2b.

We note that when measuring quantum states a homodyne detection scheme is necessary to combine the quantum signal and local oscillator. However, in this experiment our goal was to measure *optical vacuum states* and therefore no actual quantum signal needed to be combined with the local oscillator at this time. This implies that the shot-noise from the local oscillator could be directly measured by a single photodiode, without the need of a beam-splitter and photocurrent subtraction[4]. The choice of the scheme in Fig 5.2b is further justified by looking at the system from another perspective. The number of photons per unit of time, and thus the optical power of a coherent state is governed by a Poisson distribution, which equals a Gaussian distribution in the limit of $n_p \to \infty$, where n_p is the number of photons. Therefore, the probability distribution of the number of photons at the photodiode can be written as

$$\mathrm{P}_{n_p} = \frac{e^{-\bar{n}_p}\bar{n}_p^{n_p}}{n_p!}, \tag{5.1}$$

and it can be well approximated in our case ($n_p \sim 10^{14}$ photons/s) with the following Gaussian distribution

$$\mathrm{P}(x) = \frac{e^{-(x-n_p)^2/(2n_p)}}{\sqrt{2\pi n_p}}, \tag{5.2}$$

where here the variable x could be interpreted as the voltage scale in the oscilloscope or analog-to-digital converter. In Fig. 5.3 we illustrate the two schemes, the first

[3]The material used is a Rogers RO4350, characterised by a $\epsilon_d = 3.5$ dielectric constant instead FR4 ($\epsilon_d = 4.5$). The lower dielectric constant would reduce the parasitic capacitance to enhance the speed of the electronics. The main limitation was not due to the material itself but to the fact that the PCB ws designed without a golden layer on the pads for the wirebonds. The wirebonds had then to be fixed manually to the PCB using silver epoxy. This procedure proved to be extremely cumbersome and inaccurate for the scope.

[4]The photocurrent subtraction is useful to eliminate the intensity noise present in the laser light [99], which could be potentially dominating the quantum shot-noise. At this stage we ignore this aspect. It will be considered in Section 5.5.2.

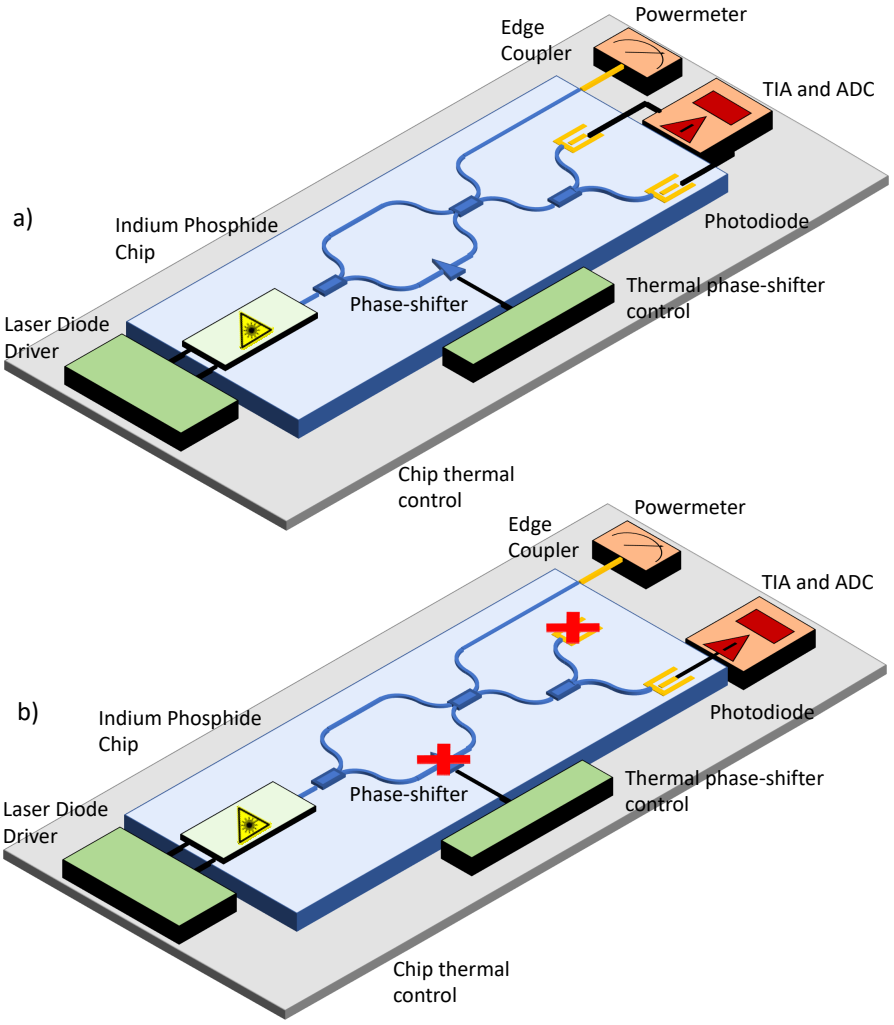

FIGURE 5.2: ***InP chip used in the experiment.*** *a) Intended diagram for a fully integrated homodyne detector, where all the components are integrated onto a single InP device. The laser diode is coupled into a MZI interferometer, composed of two MMIs and a thermal phase-shifter. One of the outputs of the MZI interferometer is coupled off-chip and the optical power is measured with a powermeter. The second output is coupled into an integrated homodyne detector (where the transimpedance amplifier and the ADC are off-chip). b) Illustrated capabilities that are not available at present. Red crosses: One photodiode was irreversibly damaged due to wrong biasing at the initial stage of the experiment. The phase shifter inside the MZI was found not to work, probably due to faulty wire-bonds between the optical chip and the electronic printed circuit board. As a consequence, the photocurrent is directly amplified by the TIA, and there is no photocurrent subtraction. Moreover, given that we could not tune the splitting ratio at the MZI, the amount of optical power directed to the photodiode is not optimised.*

using a standard balanced detector and the second directly measuring the shot-noise by filtering and amplifying the photocurrent (see Chapter 3).

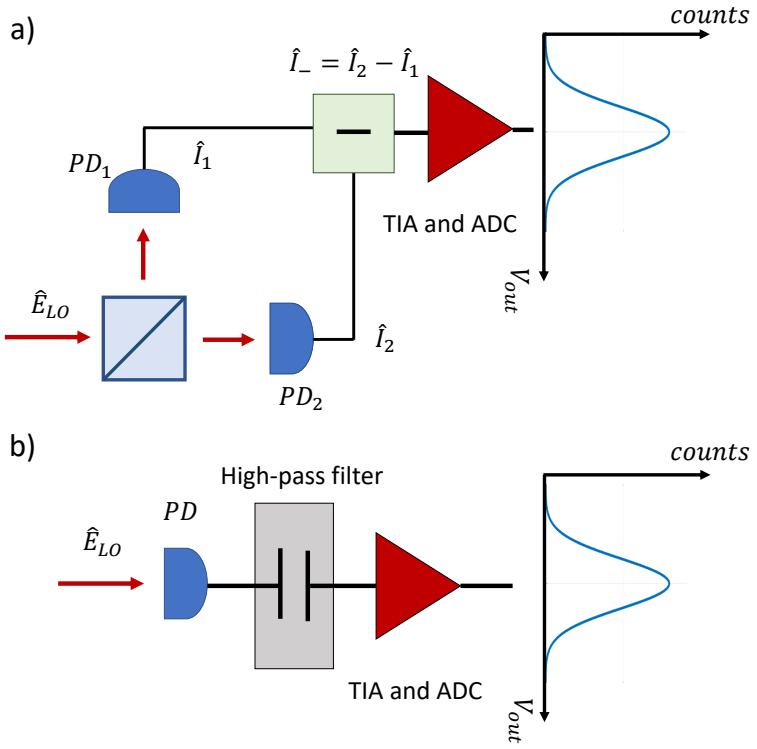

FIGURE 5.3: ***Homodyne detection scheme vs single photodiode.*** *a) Standard approach to generating random numbers based on homodyne detection. A balanced detection configuration provides a means of combining the local oscillator with an optical signal, and it has the advantage of eliminating intensity noise present in the laser light [99]. b) Scheme actually used in this experiment where the shot-noise is measured by a single photodiode, similar to [40]. Given that the intensity noise from the laser is not eliminated, it must be quantified to estimate the contribution of the quantum and classical noise present in the optical signal.*

In addition we note that this analysis is similar to the description in [40], where the authors exploit natural light detected by a phone camera to generate random numbers. It is important to note that the analysis above takes into account the ideal situation where the only noise present in the laser light is the shot-noise.

However this is not the case as many different sources contribute to the overall noise

of the laser light [99]. In particular, *intensity noise*, whose variance scales quadratically with the optical power of the emitted light, might become dominant at high optical powers. The balanced detection configuration naturally limit the intensity noise by subtracting the photocurrent generated by the photodiodes[5]. When working with a single photodiode this is not possible. Therefore, the contribution of the intensity noise to the overall noise must be quantified and taken into account when estimating the amount of quantum randomness present in the signal. Fortunately, this can be done by observing that while the variance of the quantum shot-noise scales linearly with the optical power[6], the variance of intensity noise scales quadratically with the optical power. As a result, by fitting the variance of the measured electronic signal as a function of the optical power it is possible to determine the nature of the measured signal, and thus estimate the extractable randomness. This analysis was performed on the experimental data and it will be described in Section 5.5.2.

5.4 Characterisation of the photonic chip

The highly monolithic nature of this device strongly determines the degrees of freedom available to characterise the device itself. As it can be observed by Fig. 5.2b, the laser cannot be decoupled from the MZI. Therefore, any losses in the integrated MMIs and phase-shifters constituting the MZI would simply reduce the measured optical power emitted by the integrated laser. The MZI presents two outputs, the first leading to an edge coupler for measuring the optical power off-chip, the second leading to the integrated MMI and photodiodes. Thus, the system composed by the laser and the MZI cannot be practically decoupled from either of these components. Furthermore, since no test structures to test the edge couplers are present in the chip, and the coupling power of these components strongly depend on measurement

[5]The *Common mode rejection ratio* (CMRR) of a homodyne detector describes the ability of the homodyne detector of eliminating the sources of noise common to both photodiodes as the optical intensity noise. The CMRR is usually of the order of 25-60 dB for standard balanced detectors.

[6]See Chapter 3 or for example [22].

conditions, it is difficult to estimate precisely the coupling losses and hence the optical power of the laser. Similarly we have to consider the integrated photodiodes as a single system with the laser diode and the MZI. This is because we do not have a reliable way to test them independently from the laser.

To generate random numbers by using homodyne measurements of optical vacuum states, the most important parameter is the achievable signal to noise ratio that sets the extractable randomness, through the estimation of the min-entropy. The confirmation about the *quantum* nature of the random numbers generated lies on the linearity between the optical power detected by the photodiodes and the variance of the measured optical shot-noise. Therefore, as described in Chapter 3, a linear relation between the optical power and the shot-noise variance combined with a positive signal-to-noise ratio should be a guarantee of the *quantumness* of the random numbers.

5.4.1 Characterisation of the laser linearity and threshold current

First, we characterised the integrated laser diode. Although there was a high uncertainty on the coupling losses between the optical chip and the fibres, it was possible to measure the lasing threshold of the laser and observe the linearity between the optical power and the injected input current. In Fig. 5.4 we report the optical power measured (expressed in arbitrary units because of the high uncertainty on the coupling losses) by an external powermeter as a function of the current injected into the laser diode. It can be observed that the lasing threshold is at around 11 mA and that the laser operates linearly throughout the entire input current range of the laser diode controller (0-35 mA). Some experimental data seem not to match the linear fit. This can be ascribed to the fact that the measurements were taken with a bare cleaved fibre edge coupled to the chip. This is likely to have induced small changes over time in the optical power coupled off-chip. However, as we can observe

by the table in Fig. 5.4b there is good agreement between the linear fit and the experimental data.

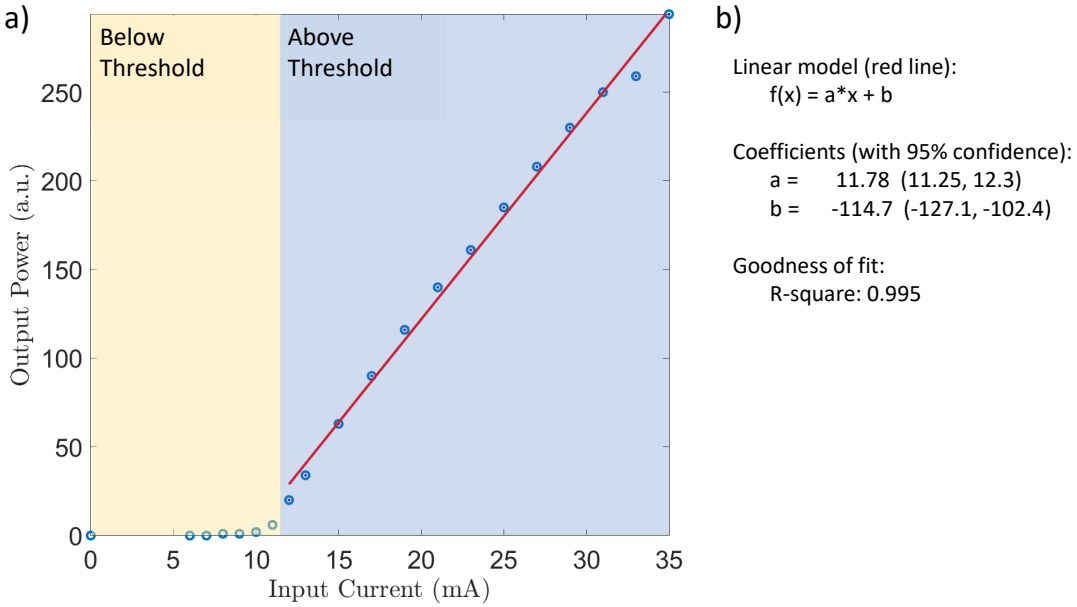

FIGURE 5.4: ***Characterisation of the InP integrated laser diode.*** *Optical power emitted by the integrated laser as a function of the input current. The optical power is measured off-chip by a powermeter. Due to the high losses and high uncertainty on the coupling losses, measured optical power is expressed in arbitrary units. However, we can observe a lasing threshold at around 11 mA and a linear behaviour throughout the entire range of the achievable input current.*

5.4.2 I-V curve of the integrated photodiodes

After characterising the integrated laser, it was then possible to characterise the integrated photodiode. The I-V curves of the photodiode were obtained by using the Keithley Sourcemeter 2450. The I-V curve characterisation of the photodiode provided information related to the reverse bias voltage required for it to operate with high responsivity and high speed[7]. Moreover, it provided us with information related to the photocurrent produced by the photodiode as a function of the input current and of the reverse bias. This step was necessary to understand how the transimpedance amplifier (TIA) for the photocurrent amplification should be

[7]Unfortunately this was used after the first attempt of biasing the photodiodes.

designed. In Fig. 5.5 we report the I-V curve for the photodiode. These results are in agreement with the specifications that suggest that the photodiode should be operated with a bias between -5 V and -10 V. From Fig. 5.5 we can see that the maximum produced photocurrent is around 80 μA. It is worth noting that in this experiment we were not able to tune the phase-shifter that controlled the optical power at the photodiode. Therefore, it is possible that with full control on the MZI the photocurrent could be increased.

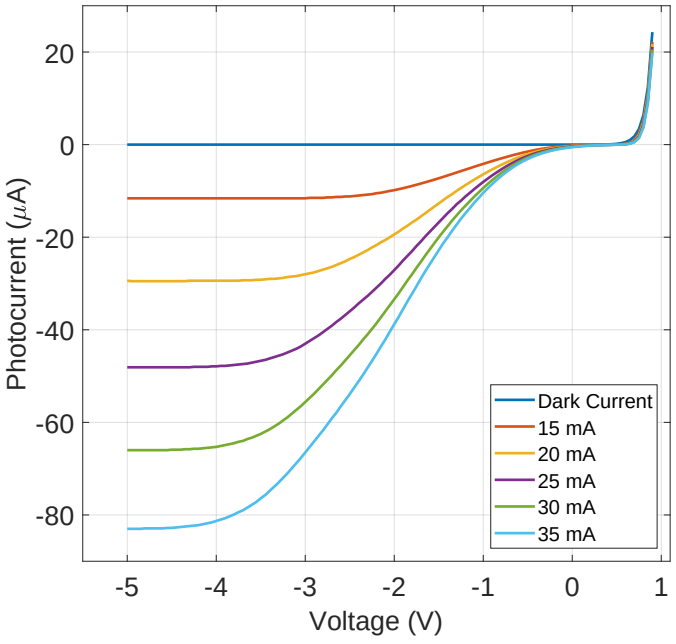

FIGURE 5.5: ***I-V curve of the photodiode.*** *Photocurrent as a function of the voltage applied to the integrated photodiode, obtained with the Keighley SourceMeter 2450. We show the data for different values of the input current. It can be observed that for a reverse bias between 0 and -4 V the emitted photocurrent is not maximised. In agreement with the specifications provided by the foundry, the photodiodes should be biased in the range -5 V to -10 V.*

5.5 Design of a TIA for the InP chip

One of the main issues encountered during this experiment lies on the specific design of the photodiodes, which are characterised by a grounded cathode terminal and a

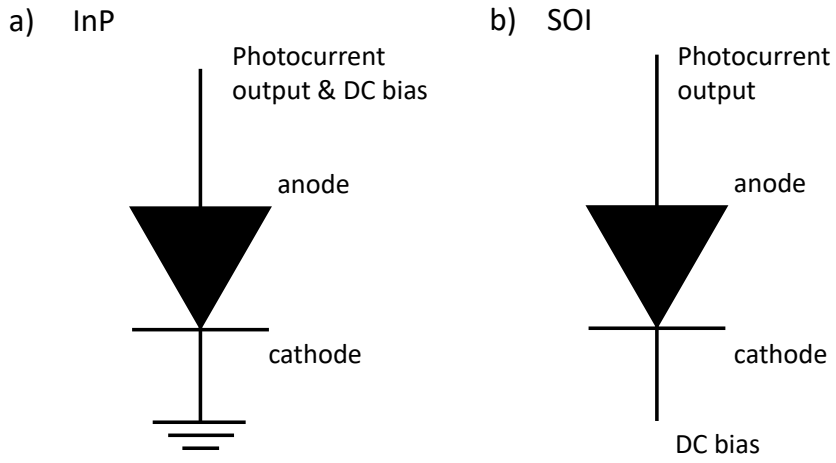

FIGURE 5.6: ***Comparison between photodiodes' designs in the InP and SOI platform.*** *a) The photodiodes in the InP chip have the anode connected to ground, while the cathode is floating. Thereofore the bias voltage is applied at the same terminal where the photocurrent is extracted. b) The SOI chip shown in the previous chapters have both floating anode and cathode. This enabled us to bias the photodiode and to extract the photocurrent independently.*

floating anode, as depicted in Fig. 5.6. This is due to the particular fabrication process provided by some InP foundries[8]. This fact has two main consequences, the first concerning the photocurrent subtraction[9] and the second related with the reverse biasing of the photodiodes[10].

Photocurrent subtraction. In Chapter 3, the subtraction between the signals is achieved by subtraction of the photocurrents. However, for the InP chip the two photocurrent have to be amplified independently by (ideally) identical amplifiers and the output voltages subtracted. This is due to the fact that both the photodiodes have a grounded cathode and therefore it would not be possible to connect the cathode of one photodiode to the anode of the second photodiode, as usually done in balanced detection. Therefore, as shown in Fig. 5.7, while in the SOI experiment

[8]This is not a fundamental limitation of the InP platform and other foundries can provide photodiodes with floating terminals [109–111].

[9]This aspect ended up being irrelevant to our experiment since we used a single photodiode. However, this is mentioned here as it presents a serious drawback of the design of these photodiodes.

[10]Moreover, the grounded cathode is part of a common ground that covers all the surface of the chip, and this fact probably affects the bandwidth of the photodiodes by adding a relatively strong capacitive effect between the terminals of the photodiode.

of Chapter 3 we performed a photocurrent subtraction, in this case we would have to subtract the voltages produced by the amplification of the photocurrents. This would have some negative consequences in terms of achievable signal-to-noise ratio. In particular, performing the voltage subtraction after the amplification stage implies that any difference in the amplifiers would reduce the quality of the subtraction, reducing the signal-to-noise ratio.

Photodiode bias. Furthermore, by observing Fig. 5.6 it can be observed that the way in which the photodiodes are reversed biased is also substantially different from Chapters 3 and 4. This is due once again to the particular design of these integrated photodiodes. From Fig. 5.6 we see that while previously we could bias the photodiode from one terminal and then collect the photocurrent at the other, in this case bias and readout are performed at the same terminal. In the two following sections we will describe two alternative approaches to target these issues.

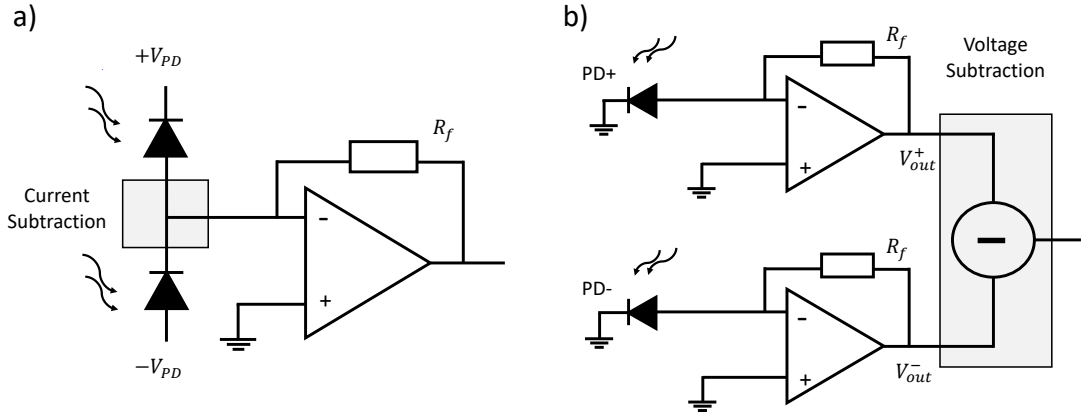

FIGURE 5.7: ***TIA comparison between SOI and InP device.*** *a) TIA scheme used in Chapter 3: photocurrent subtraction is performed before the operational amplifier, reducing the number of components required by this operation. b) Given that the photodiode has one of the terminals grounded, the signal subtraction has to be performed between the voltages in output from the operational amplifiers. (Here there is no reverse bias applied to the photodiodes and the method to supply voltage to the photodiodes is discussed in the next sections).*

5.5.1 Transimpedance Amplifier stage for the InP chip: option 1

A possible way to apply a voltage bias to the anode of the photodiode is shown in Fig. 5.8. Here, the voltage bias is applied to the non-inverting input of the operational amplifier[11]. As a result, given that the performance of the photodiode will be affected by the value at which the non-inverting input is set, the highest possible voltage operational range is required. This value is called Common Mode Input Range (CMIR) and it is usually related to the maximum supply voltage range of the amplifier. For this reason, given a relatively high voltage range supply of $\pm$ 6 V and a CMIR up to $\pm$ 4.5, we chose the OPA847 [95], the same operational amplifier used in Chapter 3. The OPA847 shows a good combination of supply voltage, low-noise and relatively high bandwidth operation. This choice has the drawback of slightly reducing the bandwidth compared to the operational amplifier (opamp) used in Chapter 4 and therefore the generation rate [112]. While other solutions could be envisaged (see Chapter 6), at this preliminary stage we chose the best known scheme in order to simplify the analysis of the experiment component by component. Given that the inverting and non-inverting inputs are at the same voltage, and the inverting input is directly connected to the anode of the photodiode, this configuration will result in a negative reverse bias of the photodiode. We designed the described transimpedance amplifier in an attempt to observe shot-noise clearance between the optical quantum noise and the electronic noise. In Fig. 5.9 we report the power spectral density measured from a single photodiode.

In Fig. 5.9 we can observe beyond 3 dB clearance between optical noise and classical electronic noise in the range 1-20 MHz[12]. This was obtained by biasing the non-inverting input with a -2.5 V. We could not bias the device with higher voltage due

[11] The technical details of why this is the case and how this scheme works can be found in Chapter 6.

[12] It can be noted that there is peak at around 60 MHz, which is a common feature of operational amplifiers when operated with relatively low feedback resistors (5kΩ is the feedback resistor we chose, as suggested by the analysis reported in [113]). It can be easily fixed by connecting a capacitor in parallel with the feedback resistor. This has not been done here since this scheme did not show good preliminary results and so we did not proceed with it any further.

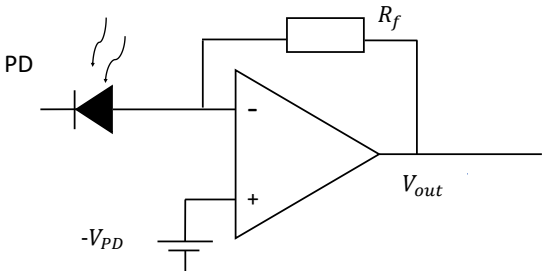

FIGURE 5.8: ***TIA scheme for the InP photodiodes.*** *The bias voltage to the photodiode is applied by setting the non-inverting input of the photodiode at a fixed voltage.*

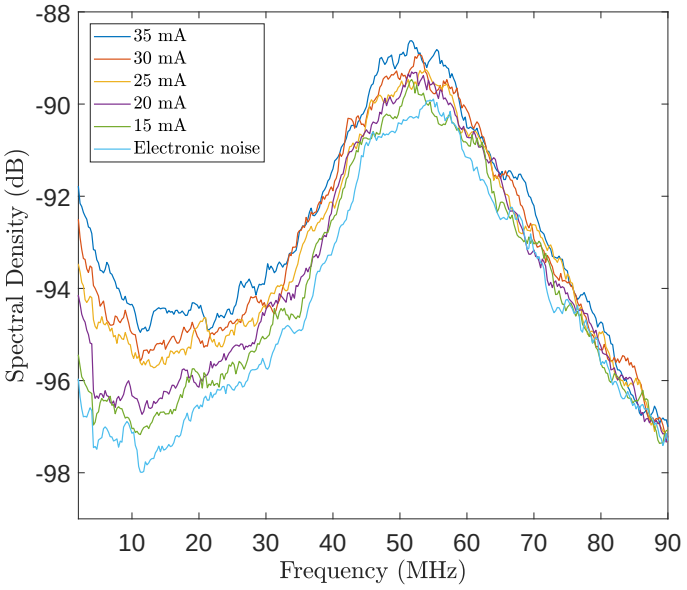

FIGURE 5.9: ***Shot-noise spectrum by biasing the non-inverting input.*** *Power spectral density of the signal from a single photodiode. At low frequencies a 3 dB shot-noise clearance between quantum signal and electronic noise can be observed. The peak at 60 MHz is a common feature of this kind of operational amplifiers and could be easily fixed by adding a feedback capacitor in parallel with the feedback resistor.*

to the fact that the direct current component of the photocurrent would saturate the operational amplifier. However, as it can be observed by Fig. 5.5, by biasing at -2.5 V we are not maximising the photocurrent generated by the photodiodes and we are below the optimal behaviour of the photodiode. A qualitative analysis of the optical powers involved shows that it would be very hard not to saturate the operational amplifier and observe the shot-noise. In fact, the voltage displacement is proportional to n_p while the voltage shot-noise standard deviation is proportional to $\sqrt{n_p}$. In our case we measured 80 μA of photocurrent (10^{14} photons/s) for a shot-noise standard deviation of 10^7 photons/s. Consequently the readout electronics should have a very high working range as well as very low noise and high resolution, with 7 orders of magnitude between them. This is very challenging and it would require extremely careful design of TIA and ADC electronics[13].

In addition, while in principle this scheme looks relatively simple, after some research among operational amplifiers and TIAs, it seems that the voltage supply range of high performance devices is too small to provide enough bias to our photodiodes. While a supply of at least -5 V is required, usually the CMIR is usually limited to $\pm$ 3.3 V for fast operational amplifiers and TIAs.

We therefore had to conclude that biasing the photodiode through the voltage applied at the non-inverting input of the operational amplifier did not yield positive results.

5.5.2 Transimpedance Amplifier stage for the InP chip: option 2

Another approach to reverse bias the photodiode was tested. This is based on a device commonly used in high-speed electronics, called bias-tee (bias-T) [114, 115]. A bias-tee is composed of an inductor and a capacitor connected in a T-shape, as in

[13] A potential solution could be a double-stage TIA where the first stage has a low gain, in order not to saturate the opamp and perform the current-to-voltage conversion. This should be followed by a high-pass filter and a high-gain inverting amplifier.

Fig. 5.10. The bias voltage is applied at the inductor terminal. The DC component (low frequency) is stopped by the capacitor which at low frequencies shows ideally infinite impedance and therefore it can travel only through the inductor. The AC component (high frequency) is stopped by the inductor which at high frequencies presents an infinite impedance and travels through the capacitor into the inverting input of the operational amplifier. We can observe that the bias-tee filters the DC current entering the operational amplifier and the signal measured in this case will not show any displacement at low frequencies. In many applications this could be an issue, but for our specific application this does not present a problem since for the random numbers we want to generate we are aiming to have a null displacement.

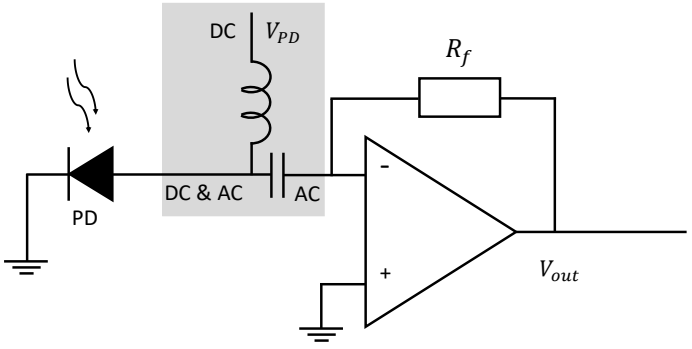

FIGURE 5.10: ***Bias-tee to bias the photodiode.*** *The reverse bias to the photodiode can be applied by taking advantage of a bias-tee. A bias-tee is composed of an inductor and a capacitor connected in T-shaped design.*

While in the ideal case a simple combination of inductor and capacitor can be used to perfectly split DC and AC component of a signal, this is not true in reality. One of the most relevant parameters for real inductors is the *Self-Resonance Frequency* (SFR), which describes the frequency beyond which capacitance effects become prevalent and the inductor does not behave properly[14]. Therefore, the actual design of a wideband bias-tee is more complex than the one sketched in Fig. 5.10. Our design is based on the bias-tee described in [115], which covers a range between several kHz and 1 GHz and whose details are reported in Chapter 6.

In the following section we report the experimental results obtained by designing a transimpedance amplifier with such a bias-tee to reverse bias the photodiode. In

[14]Details can be found in Chapter 6.

Fig. 5.11 we illustrate the spectral density obtained by measuring the amplified photocurrent out of one photodiode for different values of the input current into the integrated laser diode, similarly to Section 5.5.1. We observe a clearance between the optical signal noise and the electronic noise of 4-6 dB between 1-20 MHz. We can observe a considerable improvement in the clearance compared to Fig. 5.9. This is due to the fact that thanks to the bias-tee scheme, the voltage bias to the photodiode is completely independent from the amplification operated by the operational amplifier. Therefore we could bias the photodiode with a reverse voltage of approximate -6 V, where the produced photocurrent is almost doubled compared to a reverse bias of -2.5 V used before. Here the reduced bandwidth compared to the previous experiments is due to a non-optimised electronic circuit design (see Chapter 6).

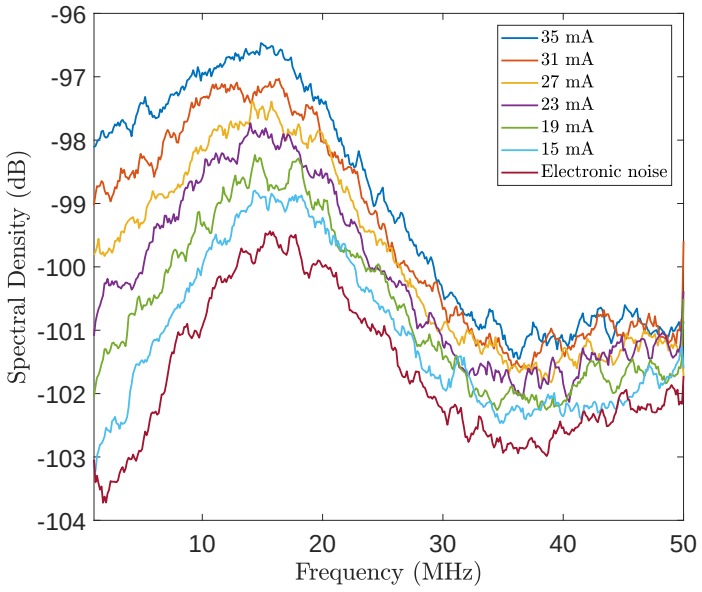

FIGURE 5.11: ***Spectrum with the measurements based on the bias-tee.*** *Power spectral density of the signal from a single photodiode, obtained with a bias-tee at the input of the TIA. In this case up to 4-6 dB clearance between optical signal and electronic noise can be observed within the TIA bandwidth of 20 MHz.*

As described in Chapter 2, there is a linear relation between the variance of the quantum shot-noise and the optical power measured by the photodiode, which would

be expressed by a line with slope $a_{id} = 1$ in a logarithmic scale. In order to verify if this condition was satisfied, we integrated the spectral density reported in Fig. 5.11 in the frequency range 1-20 MHz, for each different value of the optical power. After that, we subtracted the integral of the electronic noise obtaining, with reference to Fig. 5.11, the normalised optical noise variance. We then fitted the normalised noise variance with a line (red line in Fig. 5.12a) and reported the fit parameters in Fig. 5.12b.

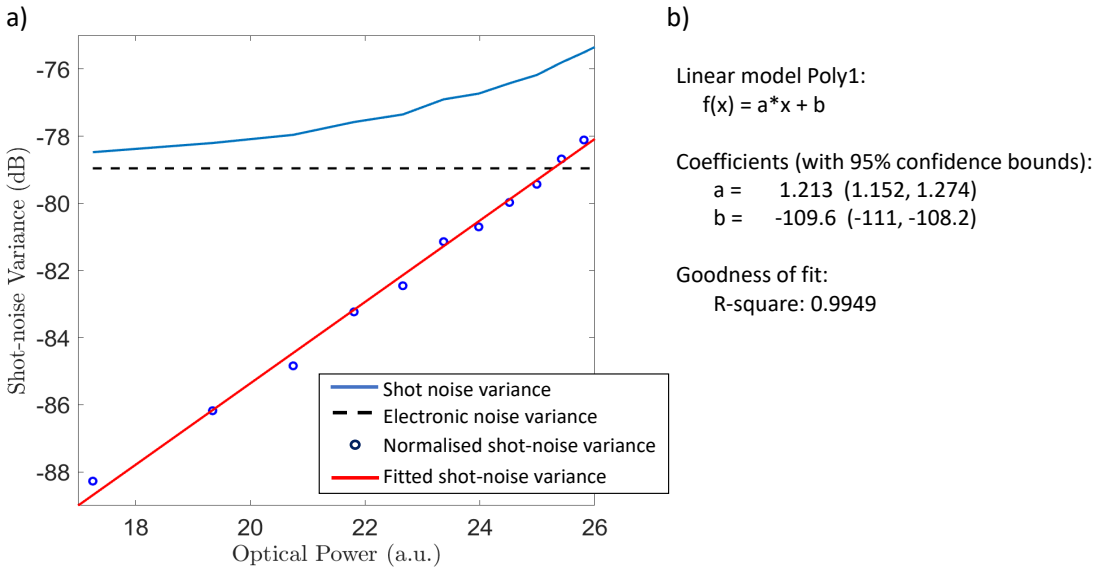

FIGURE 5.12: ***Shot-noise measurement for the InP device.*** *Noise variance of the optical signal as a function of the optical power measured by the photodiode obtained by integrating the spectral density of Fig. 5.11. It can be observed that the optical noise variance (blue line) is approximately 4 dB above the electronic noise (dashed black line). b) The normalised noise variance of the optical signal is fitted with a line of equation f(x)=ax+b. We note a discrepancy between the ideal value $a_{id} = 1$ and the measured a. This is probably due to the fact that the signal is measured from a single photodiode and not from a balanced detector. This implies that the intensity noise present in the optical signal, whose variance scales quadratically with the optical power, is not attenuated. The parameter b is a conversion factor and in this case it is arbitrary.*

In contrast with the ideal value $a_{id} = 1$, we observe that $a = 1.213$. This fact could be due to imperfections both in the optical and electronic components of the

device. On the optical side, as described in Section 5.3, the fact that we are not using a balanced detector implies that the intensity noise, whose variance scales quadratically with the optical power, is still present in the measured signal. On the electronic side, we can observe in Fig. 5.11 that the spectral response of the transimpedance amplifier is not completely flat and this could affect the output signal.

The parameter b is a conversion factor between the input current into the laser diode to the variance of the shot-noise. This was obtained by taking the laser characterisation in Fig. 5.4 and estimating the behaviour of the optical power at the photodiode. However, since we could not characterise the optical losses at the edge couplers of the chip, the optical power was expressed in arbitrary units. In addition, it is related to the specific settings of the spectrum analyser and therefore the conversion parameter b is ultimately arbitrary.

Given that we obtained a > 1, we performed a further analysis on the experimental data to extract the quantum and classical contribution from the optical signal. The following analysis is similar to the analysis performed in Chapter 4, where we estimated the ratio between the quantum phase noise Q and the other contributions (namely the classical phase noise C and the electronic noise F). In order to extract the amount of quantum shot-noise we worked in linear scale and we fitted the data with a quadratic polynomial. We then extracted the fit parameters and normalised them to the electronic noise floor. We then plotted the original curve[15] and the curve where only the linear term in the fit is taken into account (blue line in Fig. 5.13). Under the assumption that the only term that scales linearly with the optical power is the quantum shot-noise, by plotting the line described by the linear term, we should have an insight on the amount of quantum shot-noise present in the signal. We can observe that while the overall optical signal is above the electronic noise, the estimated quantum shot-noise signal is comparable but smaller than the electronic noise.

[15]This curve corresponds to the linear red line in Fig. 5.12a, but here it is expressed in a linear scale.

In principle, as long as the amount of extractable randomness can be calculated, i.e. as long as the min-entropy can be estimated, random numbers can be extracted even if the quantum noise is below the electronic noise.

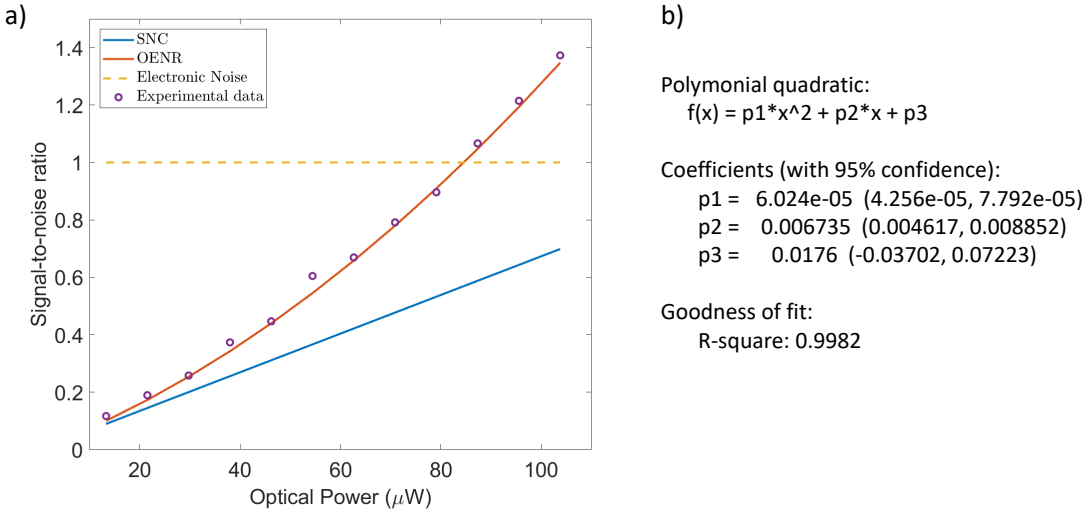

FIGURE 5.13: ***Estimation of the intensity noise and quantum shot-noise.*** *a) We report the measured variance of the total voltage noise, referred to here as optical-to-electronic noise ratio (OENR) (red line) where a quadratic behaviour can be observed. This is obtained by fitting the normalised experimental data (purple circles) with a quadratic polynomial. The blue line is the shot-noise clearance obtained by taking into account only the linear coefficient in the quadratic fit. We can observe that the variance of the quantum noise is below the level of the electronic noise of the transimpedance amplifier (yellow dashed line). b) Fit parameters for a quadratic polynomial and the optical power in the x-axis has been estimated by taking the measured photocurrent and considering a photodiode responsivity* $R = 0.8$.

5.6 Discussion and steps towards InP fully integrated QRNG

In this chapter we described the preliminary studies of a fully integrated QRNG on an InP chip. We used an integrated photodiode to measure shot-noise from an integrated laser source and we were able to observe 4 dB to 6 dB of clearance

between the optical signal and electric background noise. Because of the use of a single photodiode instead of a balanced detection configuration, the intensity noise contribution was comparable to the contribution of the quantum shot-noise. We quantified these contributions and observed that the estimated quantum shot-noise is lower but comparable to the electronic noise. This suggests that this device could be used as a quantum random number generator, after a careful characterisation of the optical signal, where the presence of intensity noise must be taken into account.

However, the initial idea of the experiment was to realise an integrated homodyne detector on an InP chip, where all the optical and opto-eletronics components were integrated onto a single device. This would be similar to the QRNG described in Chapter 3, but with the addition of an integrated laser that would massively reduce the size and complexity of the QRNG to a fully monolithic device, similarly to [41]. Unfortunately at the beginning of the experiment we encountered some issues that made us move in a slightly different direction. First, the design of the photodiodes (see Fig. 5.6) made the reverse bias of the photodiodes difficult to implement. The solution to bias the photodiodes was the design of a wideband bias-tee, which provided the required voltage bias without negative side effects. Secondly, misinterpretation of the specifications of the photodiodes meant that one of the photodiodes was damaged due to incorrect voltage biasing. Due to limited resources in terms of time and number of available copies of the same chip, we decided to investigate the feasibility of the QRNG with InP technology by characterising a single photodiode and laser. This analysis provided relevant information on how a future fully integrated QRNG based on homodyne detector should be designed.

Concluding, this particular design of the integrated photodiodes is not a fundamental issue of the InP technology, but it is due to the specific process used in some foundries. Other foundries provide chips with photodiodes in balanced detection configuration [109–111]. Therefore, future studies will involve the implementation of a fully integrated homodyne detector, to combine the features of QRNGs based on homodyne measurements of optical vacuum states with the InP platform integration capabilities. This integrated QRNG could be integrated into integrated InP

QKD devices [105].

Chapter 6

High-speed, low-noise transimpedance amplifiers

In this chapter a particular focus will be given to the amplification electronics necessary to detect the small quantum signals involved in our experiments and beyond. Throughout my Ph.D I spent a considerable amount of time in designing, testing and improving low-noise, high-speed transimpedance amplifiers (TIA). TIAs play a central role in the continuous-variable quantum information framework, as important as the generation and manipulation of quantum states. The design of the homodyne detector in Chapter 3 and sketched in Fig. 6.6 is due to Giacomo Ferranti, while I contributed to the characterisation reported in 3. I performed all the other characterisations and designs of the TIAs used during my PhD and repored in Chapters 3, 4 and 5.

6.1 Motivation

Transimpedance amplifiers are a family of electrical circuits that covert a current signal into a voltage signal. TIAs are widely used whenever a very small current must be analysed, as in the case of weak optical signals detected by photodiodes. To understand the relevance of low-noise amplification in homodyne detection, here I

quantify the magnitude of the subtracted current ($\hat{I}_-$ in Chapter 3[1]) of an homodyne detector in realistic experimental conditions. We recall that $\hat{I}_-$ is proportional to $|\alpha|$, which for coherent light is proportional to $\sqrt{n}$, where n is the number of photons detected. The optical power at the photodiodes can be written as

$$P = n_s h\nu = \frac{n_s hc}{\lambda}, \tag{6.1}$$

where n_s is the number of photons per unit of time, h is Plank's constant, c is the speed of light and λ is the wavelength. The photocurrent produced as a result of light incident onto a photodiode is therefore

$$\hat{I}_{PD} = e\eta_{PD}\frac{P\lambda}{hc}, \tag{6.2}$$

where e is the electron charge and η_{PD} is the efficiency of the photodiode. For $\eta_{PD} = 0.9$, $\lambda = 1550$ nm and P = 5 mW, the resulting photocurrent from a single photodiode is around $I_{PD} = 6$ mA and such a current can be easily analysed by a standard oscilloscope.

However, as mentioned above, when performing homodyne detection, the subtracted photocurrent between the positive and negative photodiode (hence the shot-noise signal) is proportional to the square root of the number of photons present in the local oscillator and can be written as

$$\hat{I}_- = e\eta_{PD}\sqrt{\frac{P\lambda}{hc}}. \tag{6.3}$$

By using the same parameters as above, the produced photocurrent is $\hat{I}_- = 30$ pA. In this analysis we have also to take into account a limited sampling rate of the analog-to-digital converter. Indeed the digitalised signal is obtained by multiplying the number of photo-electrons times the sampling rate. Finally the digitalised voltage signal obtained simply with a load resistor $R_L = 50\ \Omega$ would be

[1]In each experiment the photocurrent would be different, but given that the order of magnitude of the photocurrent in our experiments was comparable, this argument is useful for all the TIAs reported.

$$V_{-} \sim eR_L\eta_{PD}\sqrt{\frac{P\lambda}{hc}S}. \tag{6.4}$$

For S = 10^8 samples/s (which is a realistic parameter for bandwidths in the range of hundreds MHz), this would mean V_{-} = 1500 nV. This is roughly three orders of magnitude lower than what a standard oscilloscope can analyse.

For this reason, in order for a standard oscilloscope with a resolution of the order of 300 μV to be able to detect and analyse these low currents at high-speed, low-noise transimpedance amplifiers with a gain > 1000 need to be designed.

6.2 Transimpedance amplifiers based on operational amplifiers: ideal model

Here I will give a brief introduction on transimpedance amplifiers based on operational amplifiers. While fully integrated TIAs exist, for our prototypes we chose to use TIAs based on operational amplifiers (opamps) easily available in the market and well documented.

6.2.1 Ideal model of operational amplifiers

In order to understand the working principle of opamps, it is useful to start from an idealized model of operational amplifiers [116]. An opamp can be thought as active device that generates at the output V_{out} a voltage signal proportional to the difference between two input terminals V_1 and V_2 (see Fig. 6.1).

The *open-loop gain* A is defined as the ratio between V_{out} and the difference between V_2 and V_1. The primary assumption of the ideal model of operational amplifiers is A = ∞ from which other assumptions can be directly derived. The assumptions of an ideal operational amplifier are reported in Table 6.1.

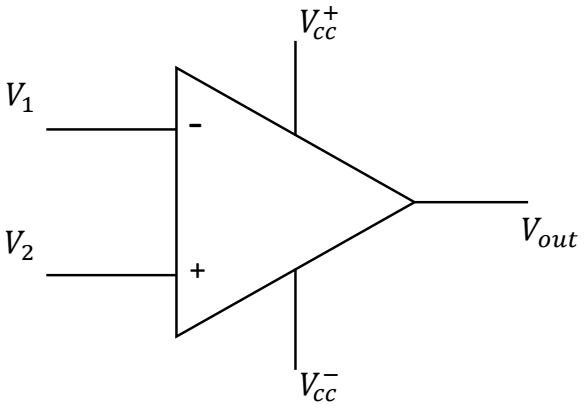

FIGURE 6.1: ***Ideal model of an operational amplifier.*** *V_1 and V_2 are called respectively inverting and non-inverting input.* $V_{cc}^{\pm}$ are the positive and negative voltage supplies and V_{out} is the output signal.

Parameter	Ideal Value
A	∞
V_{OS}	0
$I_{b_{1(2)}}$	0
Z_{in}	∞
Z_{out}	0
CMRR	∞
Bandwidth	∞

TABLE 6.1: ***Parameters of an ideal model of an operational amplifier.*** *When designing devices that involve operational amplifiers, is always useful to start from the ideal model of operational amplifiers.*

As a first approximation, which follows from the infinite open-loop gain, we have $V_2 - V_1 = 0$[2]. Intuitively, this is required to have a finite V_{out}. $I_{b_{1(2)}}$ are the input currents at the inverting and non-inverting inputs of the opamp, while Z_{in} and Z_{out} are the input and output impedance of the operational amplifier. Other important parameters are the CMRR (Common Mode Rejection Ratio), which describes the ratio between the open-loop gain A and the *common mode gain*, which is the difference between the gains of the inverting and non-inverting gains. Finally, the bandwidth in first approximation is infinite.

[2]We note that this assumption was used in Section 5.5.1 when we biased the photodiode by applying a voltage to the non-inverting input of the opamp.

6.2.2 Inverting Amplifier

Very often TIAs are based on a particular configuration of the so called *inverting amplifier*. The scheme of an inverting amplifier is reported in Fig. 6.2.

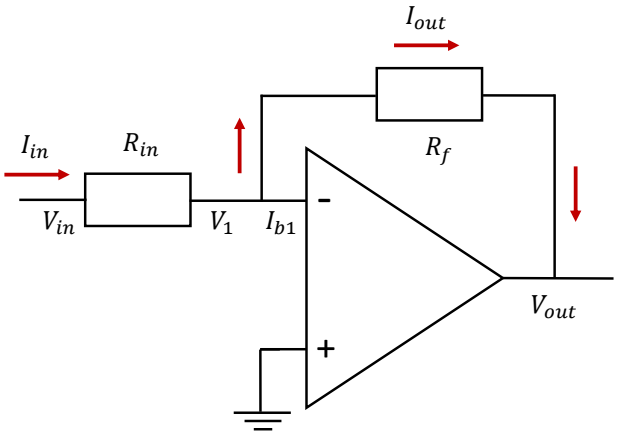

FIGURE 6.2: ***Inverting Amplifier.*** *The operational amplifier is used in inverting configuation. Here the gain and bandwidth are set by the ratio between* R_f *and* R_{in}.

For an ideal opamp we have $V_1 = 0$. This is because $V_{OS} = 0$ and because the inverting input is connected to ground. Therefore we have that $V_{in} - I_{in}R_{in} = 0$. On the other hand we have $V_1 - I_{out}R_f = V_{out}$. However, given that $V_1 = 0$, the output current $I_{out} = -V_{out}/R_f$. Also, given the infinite input impedance of the operational amplifier, $I_{out} = I_{in}$, as $I_{b_1} = 0$. Finally, defining the gain $G = V_{out}/V_{in}$, we obtain that the gain of an operational amplifier in inverting configuration is given by the ratio between the feedback resistor R_f and the input resistor R_{in}, $G = R_f/R_{in}$.

6.2.3 Opamp based TIA

As previously mentioned, TIAs based on opamps are obtained with a little variation, reported in Fig. 6.3, of the inverting amplifier scheme. Considering a current source that generates I_{in}, the TIA configuration is obtained by setting $R_{in} = 0$. In that

case $V_{in} = V_1$ and the system is described by the equation

$$V_{out} = -I_{out}R_f.$$

In this case we have a *transimpedance gain* which is given by R_f and converts the input current into an output voltage signal and whose units are V/I (or Ω).

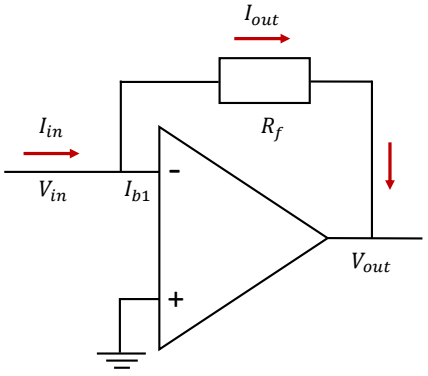

FIGURE 6.3: ***TIA based on operational amplifier.*** *The operational amplifier is used as a transimpedance amplifier. Here the gain is set by* R_f.

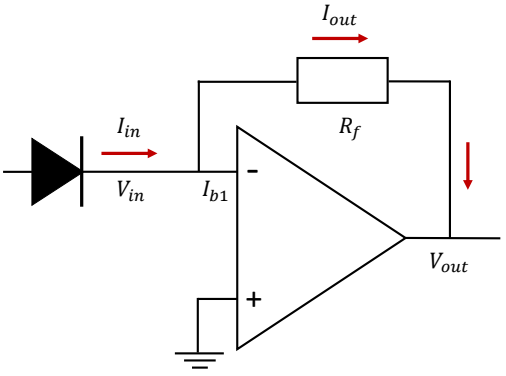

FIGURE 6.4: ***Schematic of an ideal TIA.*** *A photodiode is connected to the inverting input of an opamp. A feedback resistor* R_f *sets the transimpedance gain. The non-inverting input of the opamp is connected to ground.*

6.3 Transimpedance amplifiers based on operational amplifiers: realistic model

The analysis described in the previous section is a useful starting point to understand the basic working principle of transimpedance amplifiers based on opamps. However, when designing a real transimpedance amplifier based on opamps, we have to move beyond the ideal model and features such as the **electronic noise** and the **bandwidth** must be taken into account.

6.3.1 Electronic Noise

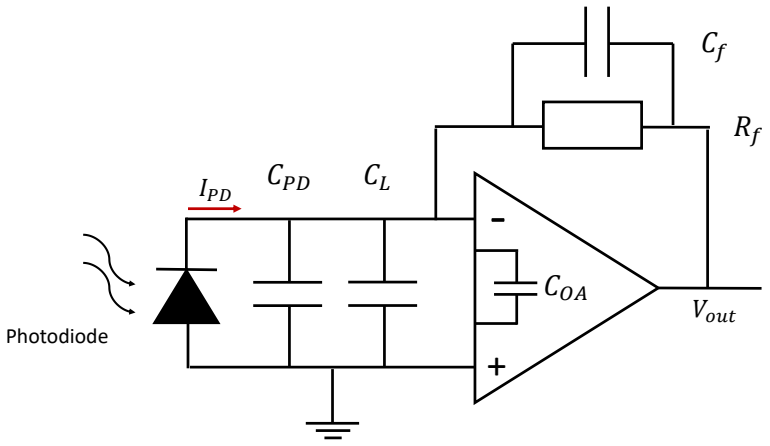

FIGURE 6.5: ***Scheme of a generic transimpedance amplifier and capacitances.*** *Here a scheme of a transimpedance amplifier is shown, including the capacitances affecting the bandwidth of a transimpedance amplifier. C_{PD} is the intrinsic capacitance of the photodiode, C_L is the contribution to the capacitance due to the physical layout of the printed circuit board. C_{OA} is the sum of the commod mode and differential capacitance of the opamp used. C_f and R_f are respectively the feedback capacitance and resistance.*

The electronic noise ultimately sets, together with the efficiency of the photodiodes (see Chapter 2), the signal-to-noise clearance (SNC) and therefore the quality of the measurement of a quantum signal. For example, when detecting single photons with homodyne detection, an efficiency $\eta > 0.5$ is necessary to observe the negativity in the Wigner function (see Chapter 2).

The electronic noise has different sources [116]:

- **Electrical Shot Noise** associated with the current flow. It is the result of charges crossing a potential barrier and it has random nature. Shot noise is characterised by a flat spectrum.
- **Thermal Noise** due to thermal agitation of electrons in a conductor. It is present in all passive elements, and it is therefore main contribution to noise in transimpedance amplifiers, due to the feedback resistor. As well as the shot noise, thermal noise is characterised by a flat spectrum.
- **1/f Noise** present in all active devices and caused by DC currents. As the name suggests, the 1/f noise decreases linearly with the frequency and it is dominant for frequencies below 100 kHz.

Usually noise in opamps is given as a contribution from the *voltage noise density* e_n, measured in $\mathrm{nV}/\sqrt{\mathrm{Hz}}$, and a contribution from the *current noise density* i_n expressed in $\mathrm{pA}/\sqrt{\mathrm{Hz}}$.

It can be shown ([116]) that for a transimpedance amplifier the overall output voltage density noise can be written as

$$e_{tot} = \sqrt{e_n^2 + i_n^2 R_f^2 + 4kTR_f}, \tag{6.5}$$

where T is the temperature, $k = 1.38 \times 10^{-23}$ JK^{-1} is the Boltzmann constant and R_f is shown in Fig. 6.4. In order to obtain the noise measured over a certain bandwidth, e_{tot} must be multiplied by the square root of the bandwidth so that

$$V_n = e_{tot} \times \sqrt{f_{max} - f_{min}}.$$

These results are valid under the assumption of constant noise and for a flat bandwidth. The assumption of flat bandwidth can be satisfied with a fairly high degree.

Both the e_n and i_n are dependent on the frequency, and therefore a precise analysis of the total noise should be obtained by integrating the noise density over the spectrum of the operational amplifier.

6.3.2 Bandwidth

The bandwidth sets the maximum achievable speed of the device. When measuring a quantum signal, it defines the maximum bandwidth of the signal that can be efficiently measured by a homodyne detector. In the context of QRNG it sets the maximum sampling rate and therefore the ultimate limit of the generation rate. Usually a compromise is necessary between electronic noise and bandwidth and the choice on which parameter should be optimised depends on the specific application. The bandwidth of a transimpedance amplification circuit is mainly affected by the capacitances of the electronic components involved (see Fig. 6.5). For TIAs based on opamps its value is given by [113]:

$$f_{-3dB} = \sqrt{\frac{GBP}{2\pi C_{tot} R_F}}, \tag{6.6}$$

where GBP is the gain-bandwidth product of the opamps and R_F is the feedback resistor. C_{tot} is the equivalent capacitance of the circuit, ideally obtained as the sum of the intrinsic capacitances of the photodiodes C_{PD}, and the differential C_D and common mode capacitance C_{CM} of the opamp ($C_{OA} = C_D + C_{CM}$). The printed circuit board (PCB) hosting the components can also introduce a parasitic capacitance C_L, which is dependent on the geometry of the design and that must be taken into account when working at bandwidths above a few MHz.

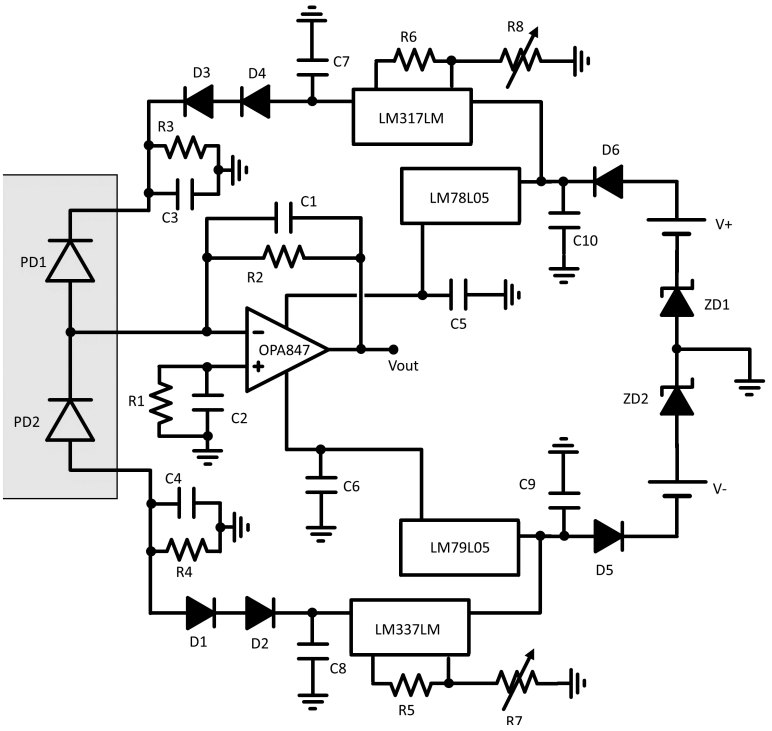

FIGURE 6.6: ***Schematic of the electronics.*** *The amplification stage of our detector was based on an OPA847 operational amplifier used in a TIA configuration. The photodiodes were integrated on the silicon chip and wire-bonded to the PCB with the electronics. R2 is the feedback resistor, which sets the gain of the TIA, and determines the bandwidth of the homodyne detector.*

6.4 Design of the balanced detector for optical vacuum and coherent states

For the experiment in Chapter 3 the homodyne detector was based on the design developed in [87]. The choice for this opamp was due to the very low voltage density noise and relatively gain bandwidth product (GBP). Fig. 6.6 shows a schematic of the electronics: the subtraction signal generated by the two photodiodes (PD1 and PD2) was amplified by a OPA847 (see ref. [95]) opamp in transimpedance configuration. The supply voltages were stabilised by means of two fixed voltage regulators (LM78L05 and LM79L05). Each photodiode was reverse-biased with a voltage provided by an adjustable voltage regulator (LM317LM and LM337LM). These two voltages were independent and could be tuned by changing the values of

the resistors R7 and R8, this to control the time response of the photodiodes. For the acquisition of the data reported in Chapter 3, both photodiodes were biased at 1 V. R_1 and C_2 served to correct for a possible voltage offset between the inverting and non-inverting inputs of the operational amplifier. The value of R_1 was chosen to be equal to R_f. The device was powered by two 9 V batteries (V+ and V-) to avoid power supply instabilities and reduce the size of the system. The ground signal was carried on the board by the external shielding of the output SMA cable and provided by the same instruments used to measure the output signal.

This homodyne detector showed a bandwidth of 150 MHz and $SNC \sim 11$ dB. Here the main limitations in terms of bandwidth were due to the opamp itself. Indeed, the quoted values for the common-mode and differential capacitances of the OPA847 were respectively 1.7 pF and 2.0 pF [95], while the feedback resistor is $R_F = 4.7$ kΩ. The quoted bandwidth of each integrated photodiode was 23 GHz [53], which corresponds to an intrinsic capacitance of $C_{PD} \sim 0.2$ pF. Assuming the parasitic capacitance of the PCB was negligible, we would expect a bandwidth of ∼180 MHz. Moroever given that measured bandwidth was f_{-3dB} ∼150 MHz this means that the estimated parasitic capacitance of the PCB was ~ 2 pF.

6.5 Design of the transimpedance amplifier for phase fluctuations QRNG

On one hand the detector described in the previous section shows low noise that allows the detection of small photocurrents with a high SNC. On the other hand, this detector suffers bandwidth limitations. As expressed by Eq. 6.6, the 3 dB bandwidth of a transimpedance amplifier is defined by the Gain Bandwidth Product (GBP) of the opamp used, by the feedback resistor R_f that determines the gain of the amplifier and by the equivalent capacitance of the system C_{tot} at the input of the opamp. The maximum achievable bandwidth by using the OPA847, is 180 MHz when using the integrated photodiodes provided by IMEC. Even in the ideal case of a PCB with

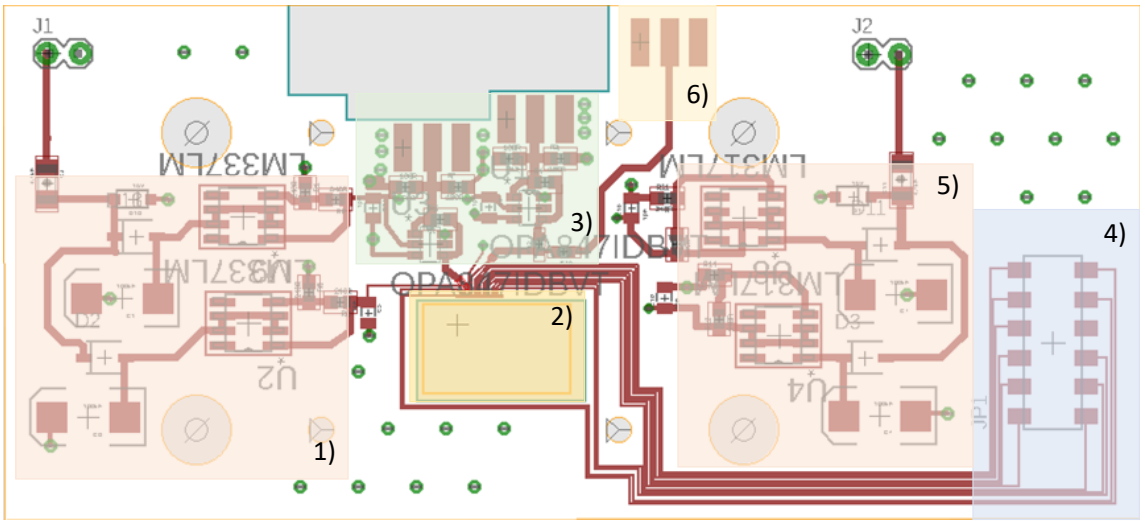

FIGURE 6.7: ***Eagle software design of the electronic board for the phase fluctuations experiment.*** *1) Negative voltage regulators for the opamps and photodiodes, including decoupling capacitors and resistors to set the voltages. 2) Area where the photonic chip is glued and pads for wirebonding the electrical connection in the photonic chip to the pads in the PCB. 3) TIAs and output SMAs for the fast signals. 4) DC connectors to control the heater drivers. 5) Positive voltage regulators for the operational amplifiers and photodiodes, including decoupling capacitors and resistors to set the voltages. 6) Output SMA for the monitor photodiode. The size of the entire PCB is about* 4×8 *mm*

null capacitance, the common mode and differential capacitance of the OPA847 are not negligible. Given that the bandwidth limits the maximum sampling rate in quantum random number generators, an alternative solution had to be researched to improve the generation rate. In the context of low noise opamps, a possible solution is given by the LT6268-10 operational amplifier by Linear Technology [112]. The LT6268-10, while keeping similar performance in terms of noise compared to the OPA847, shows characteristic input capacitances almost one order of magnitude smaller. Therefore, if associated with a good layout to reduce the parasitic and stray capacitances and photodiodes with small capacitances as the ones provided by IMEC, the use of a LT6268−10 could bring a good advantage in terms of bandwidth, without compromising the SNC. In Table 6.2 the main characteristics of the two opamps are reported.

Parameter	OPA847	LT6268-10
GBP	3.9 GHz	4.0 GHz
Common Mode Capacitance	1.7 pF	0.45 pF
Differential Capacitance	2.0 pF	0.1 pF
Input Current Noise Density	2.5 pA/$\sqrt{\text{Hz}}$	7.0 fA/$\sqrt{\text{Hz}}$
Input Voltage Noise Density	0.85 nV/$\sqrt{\text{Hz}}$	4.0 nV/$\sqrt{\text{Hz}}$

TABLE 6.2: ***Comparison between OPA847 and LT6268-10***. *In this table the main features of the two different operational amplifiers are shown. While the GBP is similar for these two devices, the lower capacitances of the LT6268-10, entails faster transimpedance amplification schemes. These specification are taken respectively from [95] and [112].*

Therefore, to improve the generation rate of our QRNG we developed a transimpedance amplifier based on the LT6268-10. When designing this detector we simulated the behaviour of the TIA by using the simulation software LTspice, reported in Fig. 6.8. This was extremely useful to select the optimal values of R_f and C_f. In particular, the bandwidth resulting from the simulation was very similar to the experimental one (Fig. 4.8), as well as the ratio between the quantum signal and the electronic background. The differences between the simulation and the experimental results were mainly due to the difficulties in estimating the parasitic capacitances involved. The characteristic capacitances of the opamp and of the photodiodes are comparable with the intrinsic capacitance of the printed circuit boards (PCB) where the electronic components have been soldered. Moreover, the characterisation of these parasitic capacitances is in general not practically easy. The design of the TIA based on the LT6268-10 is very similar to the design shown in 6.6, with minimal differences. In Fig. 6.7 we reported the Eagle[3] design of the PCB.

[3]Eagle is the software we used to design the PCBs.

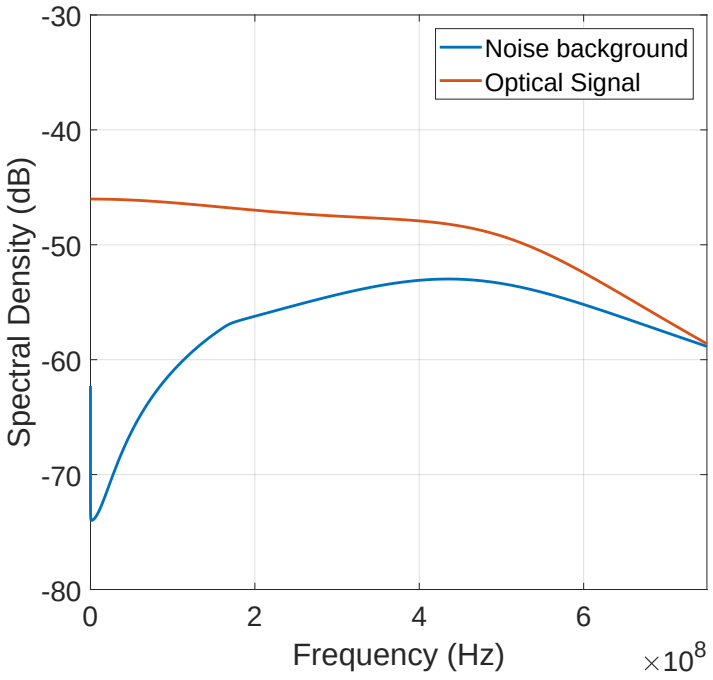

FIGURE 6.8: ***LTspice simulation of the TIA.*** *Here we report the results of the LTspice simulation for the transimpedance amplifier based on the LT6862-10. In red the optical spectral density of the quantum signal. In blue the spectral density of the electronic background noise.*

6.6 Design of a TIA for the InP QRNG

In this section I will report a few observations related with the TIA built for the InP QRNG. In principle the electronics for this device could be exactly the same as the one employed in Chapter 3 or 4. However some modifications were necessary in this case. The main reason for these changes lies in the design of the integrated photodiodes as the photodiodes in the InP chip had the anode grounded. As a consequence the usual current subtraction scheme commonly used in homodyne detectors was not possible anymore. Therefore in the design we adopted two equal but independent TIAs to amplify the positive currents, and digitally subtracted the voltage signals by making use of an oscilloscope[4]. This would had the effect of increasing the electronic noise of the overall system. Moreover, for the same

[4]In the measurements reported in Chapter 5 we actually worked with a single photodiode and therefore we used one of the two TIAs present in the design.

reason of the anode connected to ground, the voltage bias had to supplied to the photodiodes through a bias-T filter, as shown in Fig. 6.9. This enabled us to split at the same terminal the DC voltage used to bias the photodiode and the AC photocurrent in output from the photodiode. This implied that the DC component of the photocurrent was removed and therefore not amplified. In this experiment, as in Chapter 4, the adopted operational amplifiers were OPA847. In Fig. 6.10 we show the PCBs for this experiment designed with the Eagle software.

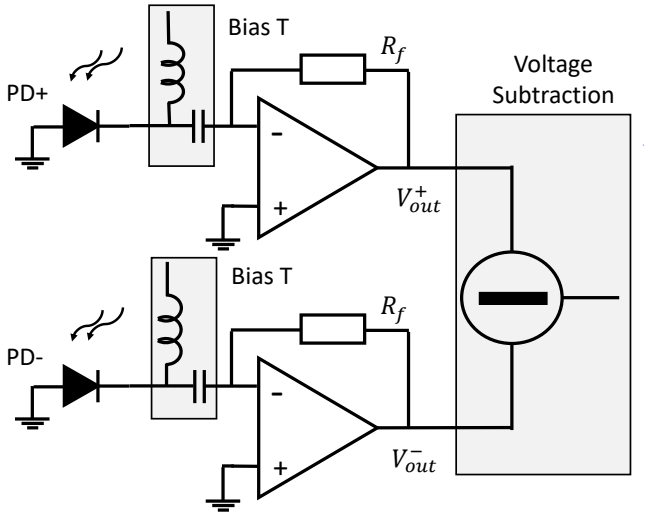

FIGURE 6.9: ***Homodyne detector for the InP QRNG.*** *We report the homodyne detector for the InP based QRNG. Here the voltage bias is supplied to the photodiodes by taking advantage of a bias-T to allow for the splitting of the DC and AC components. The subtraction is performed after two independent amplifications for the photocurrents.*

6.6.1 Design of the wideband bias-tee

Ideally the reactance of an inductor (Fig. 6.11a) can be written as

$$X_L(f) = 2\pi f L \tag{6.7}$$

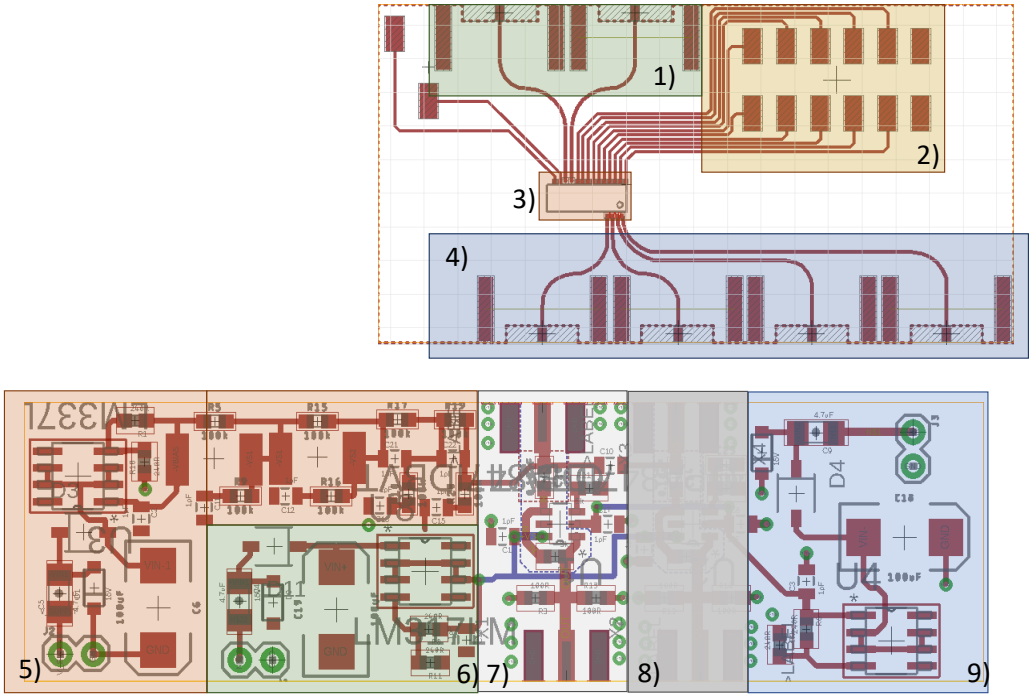

FIGURE 6.10: ***PCBs for the InP experiment.*** *The top PCB is where the InP was glued, while the bottom PCB is used to amplify the photocurrent. 1) Connector for the input current to the integrated laser diodes. 2) Low-speed electrical connection to tune integrated phase-shifters. 3) Place where the InP is glued with pads for wirebonding. 4) High-speed output connectors for the photodiodes. 5) Bias-tee to reverse bias the photodiodes. 6) Positive power supply for the operational amplifier, including decoupling capacitors and variable voltage regulators. 7) Transimpedance amplification stage including the operational amplifier, feedback resistor and passive components to operate the operational amplifier. 8) Unused TIA stage. 9) Negative power supply for the operational amplifier, including decoupling capacitors and variable voltage regulators.*

where L and f are respectively the inductance of the inductor and the frequency. A similar equation holds for a capacitor C (Fig. 6.11c), where we have

$$X_C(f) = \frac{1}{2\pi f C}. \tag{6.8}$$

It can be easily observed that while the reactance of a inductor increases with the frequency, the reactance of the capacitor decreases for high frequencies. Therefore, in the ideal case a simple bias-tee with an inductor and capacitor would succeed in

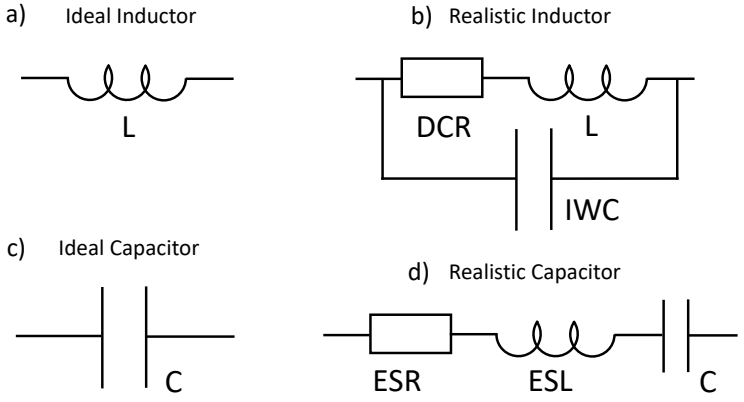

FIGURE 6.11: ***Passive components: ideal and realistic model.*** a) Ideal inductor b) Realistic inductor with parasitic inter-winding capacitance (IWC) and direct current resistance (DCR). c) Ideal capacitor. d) Realistic capacitor with equivalent series inductance (ESL) and resistance (ESR).

splitting the alternate current (AC) and direct current (DC), provided that

$$X_L(f) \gg Z_0 \qquad (6.9)$$
$$X_C(f) \ll Z_0.$$

Here Z_0 is the characteristic impedance of the electrical trace in the printed circuit board. Therefore, ideally a high value of an inductor combined with low capacitance would satisfy the requirement expressed by 6.9. However, in the real-world the behaviour of components is affected by side effects. This is the case for inductors and capacitors (Fig. 6.11b and 6.11d), where Eqs. 6.7 and 6.8 respectively become

$$X_L^{real} = DCR + \frac{X_{IWC} X_L}{X_{IWC} + X_L} \qquad (6.10)$$

and

$$X_C^{real} = \sqrt{ESR^2 + (X_C + X_{ESL})^2}. \qquad (6.11)$$

From Eq. 6.10 we observe for a realistic inductor a resonance at

$$f_{res} = \frac{1}{2\pi\sqrt{L}\sqrt{IWC}}. \qquad (6.12)$$

This is called the *self-resonance* of the inductor, and it is caused by the parasitic capacitance of a physical device. The main consequence is that for high frequencies the inductor stops behaving as an inductor and starts behaving as a capacitor. This has the consequence that the AC and DC components of the signal are not splitted anymore, compromising the functionality of the bias-tee. Therefore, the choice of the components for the bias-tee is constrained by Eqs. 6.9, 6.10 and 6.11. It turns out that for a single inductor it is hard to satisfy these conditions and it is therefore conventient to build a series of inductors in order to achieve wideband performance. In this experiment I used a design described in [115], which provides a bandwidth between 50 kHz to 1 GHz. The schematic is reported in Fig. 6.12. The results of Section 5.5.2 were obtained by using the scheme shown here.

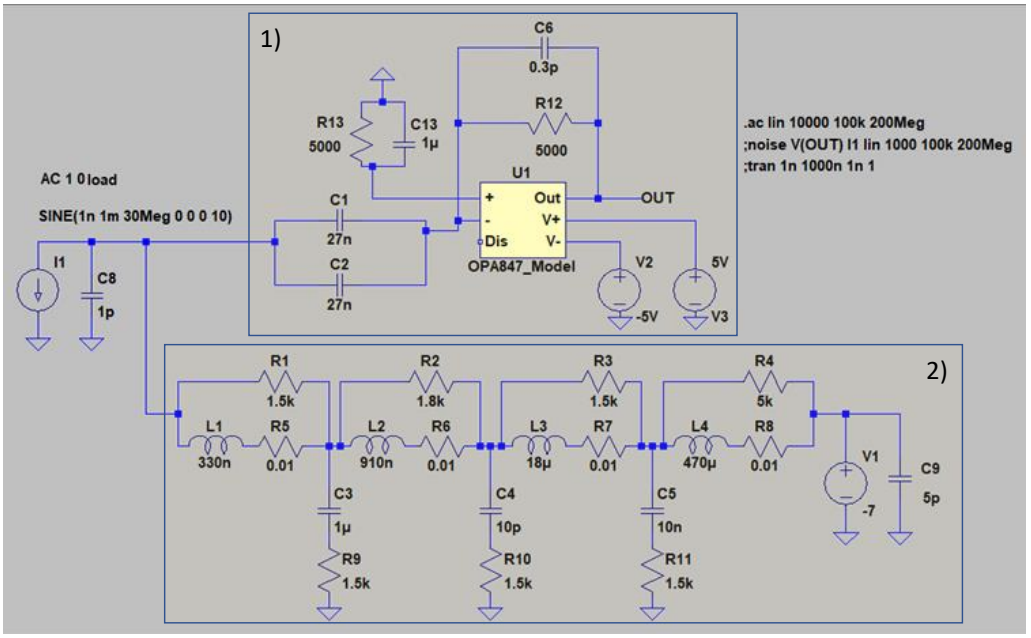

FIGURE 6.12: ***LT-spice scheme of the TIA and bias-tee.*** 1) Scheme of the TIA, similar to the scheme used for the previous experiments. 2) Bias-tee composed of four inductances in series of different values, from 300 nH to 470 μH. Each inductance is connected in parallel with a resistor to reduce oscillations. Three capacitors in series with a resistor, connected between the inductors and the ground help to flatten the spectral response of the bias-tee.

6.7 Improving the bandwidth of transimpedance amplifiers

While with OPA847, used for the experiment in Chapter 3, we almost reached its maximum bandwidth, with the LT6268-10 there is still room to improve the bandwidth, by applying some observations made previously. First of all, we noticed that the intrinsic capacitances of the printed circuit board play a relevant role in the overall speed of the detector. In Eq. 6.6 it can be seen that the lower the capacitances, the faster the detector. Given that these capacitances depend, among other factors, on the material used for the PCB, the first step is to look for a material with lower dielectric constant. For the same layout, the parasitic capacitances depend on the dielectric constant. In our particular case we used FR4 PCBs, for the main reason that this is the most common material for general PCBs, and the cheapest. In this case the dielectric constant is $\epsilon_r \sim 4.5$. However, materials such as Rogers RO4350 and Arlon 25FR, having a $\epsilon_r \sim 3.5$, should bring a considerable advantage in reducing the parasitic capacitances. For example, a simple copper trace used to connect two points on a PCB has a capacitance

$$C(pF) = \frac{0.264(\epsilon_r + 1.41)}{\ln\left(\frac{5.98h}{0.8w+t}\right)}x, \tag{6.13}$$

where w and t are respectively the width and thickness of the copper trace, while h is the height of the dielectric and x the length considered (see Fig. 6.13 for reference). From Eq. 6.13, for a trace 0.8 mm wide on a PCB high 1.6 mm as the one we used, C = 0.6 pF for an FR4 PCB. By changing the material, and hence by changing the dielectric constant we obtain C = 0.5 pF. From this simple calculation is clear that a 20% advantage could be achieved simply by a proper choice of the material [117].

It is worth stressing here that many faster transimpedance amplifiers are available. During the experiments we chose very low-noise amplifiers to have a higher SNC and to make it easier the optimisation of all the parameters that had to be taken into

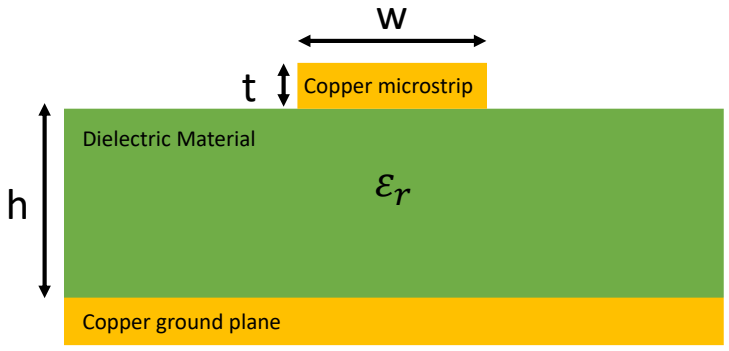

FIGURE 6.13: ***Section of a PCB.*** *The yellow stripes represent the copper trace (top) and the copper plane (bottom). w and t represent respectively the width and thickness of the copper trace, while h represents the height of the dielectric material.*

account. In Table 6.3, we listed a few possible alternative amplifiers, with similar specifications in terms of electronic noise but that could potentially outperform our current solutions in terms of bandwidth.

Model	Device	Bandwidth/ GBP	Input Capacitance	Voltage/Current Noise Density
MAX3277 [118]	TIA	2.3 GHz	0.85 pF	6 pA/$\sqrt{\text{Hz}}$
HMC799 [119]	TIA	700 MHz	$<$ 1pF	5 pA/$\sqrt{\text{Hz}}$
OPA858 [120]	opamp	5.5 GHz	0.8 pF	2.55 nV/$\sqrt{\text{Hz}}$
OPA855 [121]	opamp	8 GHz	0.8 pF	0.98 nV/$\sqrt{\text{Hz}}$
LT6409 [122]	opamp	10 GHz	0.5 pF	1.1 nV/$\sqrt{\text{Hz}}$
”	”	”	”	8.8 nA/$\sqrt{\text{Hz}}$

TABLE 6.3: ***Possible faster TIA for QRNG applications.*** *Here we list some operational amplifiers or TIAs that could be potentially used to increase the generation rates of our QRNGs. For the opamp the GBP is reported, while for the TIAs the actual bandwidth is reported. The voltage/current noise is referred always to the input, in order to have an understanding of its value it must be multiplied by the square root of tha bandwidth and the feedback resistor. Where not reported the current/voltage noise density is not relevant, and therefore it is not reported in the specsheet.*

6.8 Environmental Electronic Noise

The environmental noise was caused by all the electronic devices internal and external the lab where the experimental setup was placed. In our case the most detrimental noise was due to the FM signals that have frequencies ranging between 80 MHz to 110 MHz, plus other contributions at lower frequencies, as shown in Fig. 6.14. These radio signal, if not properly shielded, would be captured and amplified by the opamp. This would ultimately add up to the quantum signal that we wanted to measure. In the frequency domain this could be observed as peaks at some discrete frequencies. If the signal is measured in the time domain, i.e. by an oscilloscope, the environmental noise would contribute by adding periodic oscillations to the signal. When generating random numbers for example, this would add periodic correlations between the bits, strongly reducing the effective randomness.

To run the various experiments, many electronic instruments were directly connected to our device. The integrated phase-shifters were thermo-optic shifters controlled by heater drivers. These heater drivers were controlled by a desktop computer. The chip was temperature stabilised by a temperature controller. Finally the oscilloscope to digitalize the data was connected to the TIA through an coaxial cable. As a consequence, all the cables and wires connecting these instruments to our homodyne detection absorbed part of the environmental electronic noise, carrying it into the TIA. This noise, when not properly eliminated, was amplified together with the quantum signal. In Fig. 6.14 we show how the signal spectral density of the homodyne detector would look without a careful shielding of the amplification electronics. In order to be able to measure a clean signal we enclosed the chip and the transimpedance amplifier in a Faraday cage. All the cables and wires external to the cage were carefully shielded and the shielding was connected to ground. Then all these external cables were connected to the Faraday cage through the shielding layer, by making use of conducting gaskets to optimise the contact connector-cage. The cage and all the shielding of the cables were therefore connected to a common ground. Since the shielding of these cable was not perfect, we used ferrite beads to

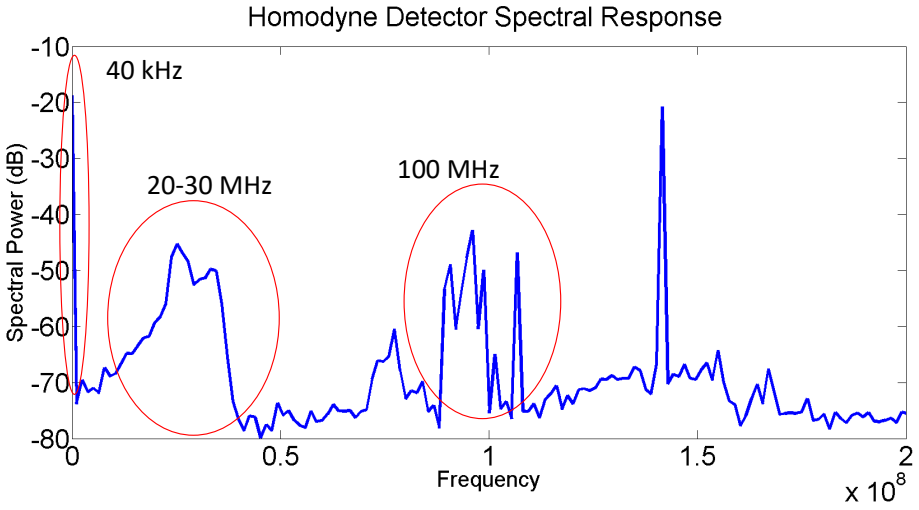

FIGURE 6.14: ***Spectral density without shielding of the electronics.*** *The spectral density of the signal measured by the homodyne detector, without proper shielding shows many peaks arise due to environmental noise. The peaks at around 100 MHz are due to the FM signal, while those at 20-30 MHz are caused by electronic components connected to the TIA.*

help reduce the high frequency noise contribution. We remark here that the signal from the heater driver to the chip as well as the signals from/to the temperature controller were low frequency signals. Therefore the high frequency signal carried by these cable was pure environmental/instrumental noise. Inside the cage the wires were properly shielded were necessary. They were also tightly twisted and kept as short as possible to reduce inductive effects. All these precautions strongly reduced the negative effects of the environmental noise on the system and using this methodology enabled collection of the results reported throughout this thesis.

6.9 Final remarks

In this chapter we discussed many aspects related with the practical implementation of the electronic amplification required for the readout of the optical signal. First we motivated the necessity for the use of transimpedance amplification schemes and gave a brief introduction on the principles behind TIAs. Second, I described the

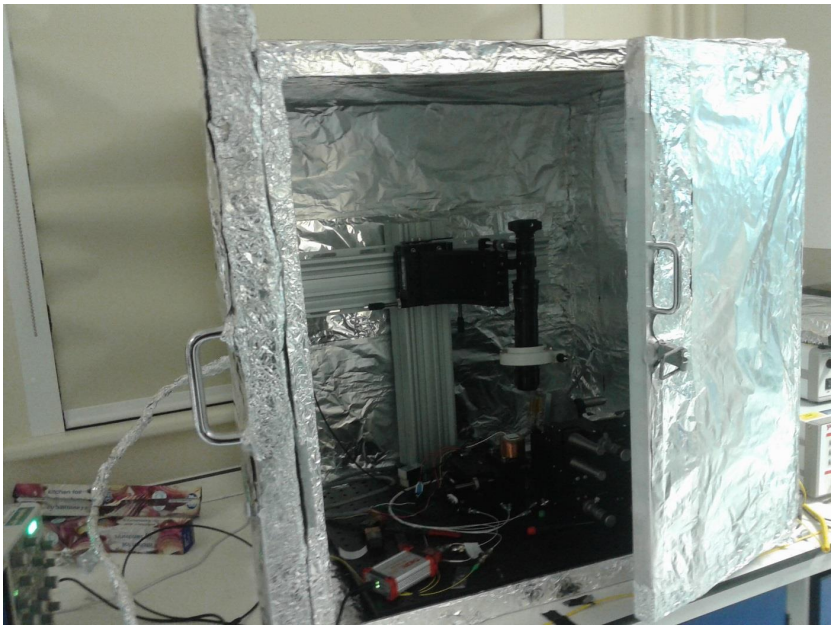

FIGURE 6.15: ***Picture of the Faraday cage.*** *The Faraday cage contains the chip and the TIA mounted on a chip rig for vertical coupling.*

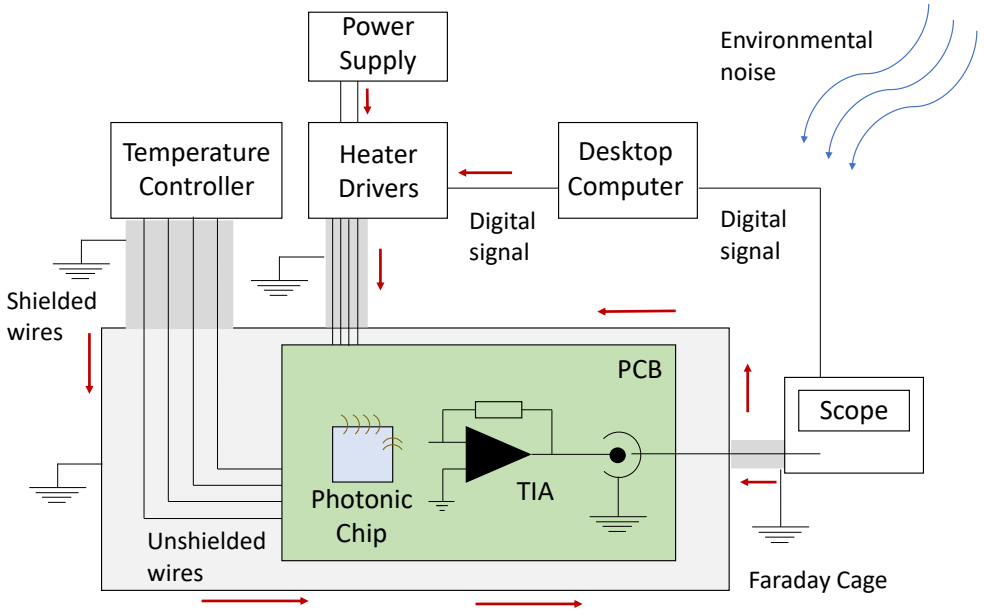

FIGURE 6.16: ***Scheme of the eletronics for the integrated TIA.*** *All the instruments used to drive the experiment are connected to the PCB holding the photonic chip and TIA. In order to minimize the environmental noise amplified by the TIA a Faraday cage has been built and care has been paid in shielding the signal cables.*

actual devices I designed and used during my Ph.D. On this subject the are many other possible solutions to explore to maximise the performance of these devices in terms of signal-to-noise ratio and achievable speed. Finally I reported some more practical issues such as the environmental electronic noise. Despite at first this might not seem a central topic, the environmental noise massively affect the electronic amplification systems used. Moreover a clever use of this environmental noise could be potentially use to hack QRNGs, by exploiting the correlations introduced by the FM noise in the voltage signal. Hence the way in which the system is isolated from the environment is extremely relevant to QRNG. Here a careful engineering of the physical device should guarantee the required protection from potential attacks.

Chapter 7

Conclusions

In this thesis I have reported different schemes for generating random numbers in integrated platforms. Our protocols take advantage of standard lasers as light sources and integrated linear optics combined with integrated photodiodes for the readout process.

Our results demonstrate that it is feasible to integrate QRNGs onto chip structures and therefore open the way to future demonstrations where QRNG modules are integrated with more complex systems, such as integrated devices for quantum communications.

In Chapter 3 we demonstrated a QRNG by building an integrated homodyne detector in the Silicon-on-Insulator platform where beam-splitter and photodiodes were integrated in the same microchip. We also showed that our device has the correct specifications to faithfully characterise quantum states. In Chapter 4 we reported a QRNG on the same SOI platform, where instead of homodyne measurements, we exploited phase fluctuations from an external laser diode. The phase fluctuations were converted into intensity fluctuations by making use of an integrated MZI with the light detected by integrated Germanium photodiodes. Since these two experiments were performed in the same photonic platform, the different performance can be ascribed to the intrinsic features of the different techniques, in relation to our specific

physical realisation. The performances of these experiments were summarised in Table 7.1. In particular, the phase noise effect is much stronger than the shot-noise of coherent light. As a result, the quantum noise extractable with the phase fluctuations methods, for the same optical power, can be orders of magnitude larger than the one obtained with homodyne measurements of optical vacuum states. This fact can be exploited in different ways. On one hand, the same amount of entropy can be extracted with much lower optical powers, provided that a similar transimpedance amplifier (TIA) is used. This is particularly relevant in integrated devices with high density of components and lower optical powers help reduce the optical cross-talk that could be potentially detrimental for the system. Alternatively, by keeping comparable optical powers, the need for low noise TIAs is removed and higher speeds can be achieved with QRNGs based on phase fluctuations. On the other hand,

Experiment	Generation Rate	Optical Power (off-chip)	Optical Power (photodiodes)	On-chip area
Homodyne	1.2 Gbps	20 mW	5 mW	0.1 mm × 0.3 mm
Phase noise	2.8 Gbps	300 μW	40 μW	1 mm × 1 mm

TABLE 7.1: ***Comparison between the SOI integrated QRNGs***. *Here the different performance and features between the SOI based QRNGs are shown. While the generation rates are on the same order of magnitude for these devices, the specifications show remarkable differences. In the phase fluctuations experiement, the Gbps regime is achieved with sub-mW optical power, one order of magnitude below the power needed in homodyne detection. However, the footprint of homodyne based QRNGs is strongly reduced compared to the phase fluctuations scheme.*

while QRNG based on phase fluctuations must be composed of trusted source and measurement devices, schemes for self-certification of QRNG based on homodyne measurements have recently been developed [28–30]. Therefore, QRNGs based on homodyne measurements can have stronger guarantees about the security of the generated random numbers. Moreover, the footprint of an integrated homodyne detector is smaller, given that the scheme based on phase fluctuations requires a long delay line which occupies a non negligible area on the chip. Therefore whenever the space available in a chip is limited, the scheme based on homodyne measurements

could provide a better solution. Each scheme shows advantages and disadvantages and either of them might be preferable depending on the specific application.

Moreover, we observe that so far both these implementations are outperformed, in terms of generation rates, by their bulk/fibre optics counterparts. This is due, in both the experiments, to specific features of our realizations and is not due to fundamental limitations of the integrated platforms used.

The InP integrated QRNG has the important advantage of an integrated laser source. This considerably reduces the complexity of the device. Our experiment showed some practical issues that partially limited the performance of our device. These issues could be resolved with further time for another attempt, and the possibility of monolithically integrating the laser source in the very same platform of the measurement device remains a very appealing option nonetheless, and is worthy of further tests and experiments. However, positive preliminary results were obtained ad reported, by measuring the shot-noise with a single photodiode. These preliminary results show the feasibility of a QRNG based on a fully integrated homodyne detector in the InP platform.

In Chapter 6 I reported technical details about the transimpedance stage which I designed and used in the different experiments. While the optical side of a QRNG (including the photodiodes) provides the *quantum* random signals, these signals are often too small to be converted into digital random bits and so an amplification stage is necessary. However low-noise, high-gain amplification at high speeds is not a trivial task and it is central to improve the performance of QRNGs. Furthermore, high specification transimpedance amplifiers play a key role in the wider field of continuous-variable quantum information.

In summary, three different approaches to generating random numbers have been explored during my Ph.D. Work in the near future will include the monolithic integration of these QRNGs into Quantum Key Distribution terminals and other integrated devices which require high-rate generation of random bits. Random numbers

play a key role in a vast range of applications and quantum random number generators are a powerful solution to provide random numbers at high rates. Furthermore QRNGs are among the most advanced *Quantum Technologies* and the recent development of integrated QRNGs, thanks to the reduction in costs and size and thanks to the possibility of producing them on a larger scale, will help build a bridge between lab demonstrations and real-world applications. Moreover, integrated QRNGs are a CMOS compatible technology and could be integrated in electronic microprocessors. We therefore expect QRNGs to find widespread applications in the near future, opening the era of quantum technologies.

Bibliography

[1] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Review of Modern Physics*, vol. 89, p. 015004, Feb 2017.

[2] C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, pp. 615–621, May 2000.

[3] J. Szczepanski, E. Wajnryb, J. Amigo, M. V. Sanchez-Vives, and M. Slater, "Biometric random number generators," *Computers & Security*, vol. 23, no. 1, pp. 77 – 84, 2004.

[4] T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-based random number generators. Part II: practical realization," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, pp. 382–385, March 2001.

[5] P. Kohlbrenner and K. Gaj, "An embedded true random number generator for FPGAs," in *Proceedings of the 2004 ACM/SIGDA 12th International Symposium on Field Programmable Gate Arrays*, FPGA '04, (New York, NY, USA), pp. 71–78, ACM, 2004.

[6] M. Hamburg, P. Kocher, and M. E. Marson, "Analysis of Intel's Ivy Bridge digital random number generator," 2012. Cryptography Research, Inc.

[7] G. Taylor and G. Cox, "Digital randomness," *IEEE Spectrum*, vol. 48, pp. 32–58, September 2011.

[8] "Evaluation of VIA C3 Nehemiah random number generator," 2003. Cryptography Research Inc.

[9] IDQuantique, "Quantis random number generator." `https://www.idquantique.com`. Accessed: September 2018.

[10] "Fast quantum random number generation." `http://www.quintessencelabs.com/our-technology/?tab=random-number`, 2014. Accessed: September 2018.

[11] "Entropy analysis and system design for quantum random number generators in CMOS integrated circuits." `https://comscire.com/files/whitepaper/Pure_Quantum_White_Paper.pdf`, 2014. Accessed: September 2018.

[12] M. Isida and H. Ikeda, "Random number generator," *Annals of the Institute of Statistical Mathematics*, vol. 8, no. 2, pp. 119–126, 1956.

[13] J. S. Bell, "On the Einstein Podolsky Rosen paradox," *Physics*, vol. 1, no. 3, pp. 195–200, 1964.

[14] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Physical Review Letters*, vol. 23, pp. 880–884, Oct 1969.

[15] J. Rarity, P. Owens, and P. Tapster, "Quantum random-number generation and key sharing," *Journal of Modern Optics*, vol. 41, no. 12, pp. 2435–2444, 1994.

[16] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Review of Scientific Instruments*, vol. 71, no. 4, pp. 1675–1680, 2000.

[17] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, "Photon arrival time quantum random number generation," *Journal of Modern Optics*, vol. 56, no. 4, pp. 516–522, 2009.

[18] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," *Applied Physics Letters*, vol. 98, no. 17, p. 171105, 2011.

[19] M. Stipčević and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," *Review of Scientific Instruments*, vol. 78, no. 4, p. 045104, 2007.

[20] H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," *Optics Express*, vol. 18, pp. 13029–13037, Jun 2010.

[21] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, "Quantum random-number generator based on a photon-number-resolving detector," *Physical Review A*, vol. 83, p. 023820, Feb 2011.

[22] A. I. Lvovsky and M. G. Raymer, "Continuous-variable optical quantum-state tomography," *Review of Modern Physics*, vol. 81, pp. 299–332, Mar 2009.

[23] A. Trifonov and H. Vig, "Quantum noise random number generator." `https://patents.google.com/patent/US7284024B1`, 2007. US Patent US7284024B1.

[24] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," *Nature Photonics*, vol. 4, pp. 711–715, oct 2010.

[25] Y. Shen, L. Tian, and H. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum states," *Physical Review A*, vol. 81, p. 063814, Jun 2010.

[26] T. Symul, S. M. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light," *Applied Physics Letters*, vol. 98, no. 23, 2011.

[27] J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, "Maximization of extractable randomness in a quantum random-number generator," *Physical Review Applied*, vol. 3, p. 054004, May 2015.

[28] D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent ultrafast quantum random number generation," *Physical Review Letters*, vol. 118, p. 060503, Feb 2017.

[29] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, "Secure heterodyne-based quantum random number generator at 17 Gbps." arXiv:1709.00685v1 [quant-ph], 2017.

[30] B. Xu, Z. Li, J. Yang, S. Wei, Q. Su, W. Huang, Y. Zhang, and H. Guo, "High speed continuous variable source-independent quantum random number generation." arXiv:1709.00685v1 [quant-ph], 2017.

[31] Z. Zheng, Y.-C. Zhang, W. Huang, S. Yu, and H. Guo, "6 Gbps real-time optical quantum random number generator based on vacuum fluctuation." arXiv:1805.08935 [quant-ph], 2018.

[32] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," *Optics Letters*, vol. 35, pp. 312–314, Feb 2010.

[33] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," *Optics Express*, vol. 20, pp. 12366–12377, May 2012.

[34] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," *Review of Scientific Instruments*, vol. 86, no. 6, 2015.

[35] J. Liu, J. Yang, Z. Li, Q. Su, W. Huang, B. Xu, and H. Guo, "117 Gbits/s quantum random number generation with simple structure," *IEEE Photonics Technology Letters*, vol. 29, pp. 283–286, Feb 2017.

[36] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, "True random numbers from amplified quantum vacuum," *Optics Express*, vol. 19, pp. 20665–20672, Oct 2011.

[37] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," *Optics Express*, vol. 22, pp. 1645–1654, Jan 2014.

[38] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," *Optics Express*, vol. 18, pp. 23584–23597, Nov 2010.

[39] A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, "Sub-Tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals," *Journal of Lightwave Technology*, vol. 30, pp. 1329–1334, May 2012.

[40] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, "Quantum random number generation on a mobile phone," *Physical Review X*, vol. 4, p. 031056, Sep 2014.

[41] C. Abellan, W. Amaya, D. Domenech, P. M. noz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, "Quantum entropy source on an photonic integrated circuit for random number generation," *Optica*, vol. 3, pp. 989–994, Sep 2016.

[42] M. Rude, C. Abellan, A. Capdevila, D. Domenech, W. M. Mitchell, W. Amaya, and V. Pruneri, "Phase diffusion quantum entropy source on a silicon chip." arXiv:1804.04482 [quant-ph], 2018.

[43] B. Haylock, D. Peace, F. Lenzini, C. Weedbrook, and M. Lobino, "Multiplexed quantum random number generation." arXiv:1801.06926 [quant-ph], 2018.

[44] A. Politi, M. J. Cryan, J. G., S. Yu, and J. L. O'Brien, "Silica-on-silicon waveguide quantum circuits," *Science*, vol. 320, pp. 646–649, 2008.

[45] A. Politi, J. C. Matthews, M. G. Thompson, and J. L. O'Brien, "Integrated quantum photonics," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 15, pp. 1673–1684, 2009.

[46] J. Silverstone, D. Bonneau, J. O'Brien, and M. Thompson, "Silicon quantum photonics," *IEEE Journal of Selected Topics in Quantum Eelctronics*, vol. 22, pp. 390 – 402, 2016.

[47] G. Lifante, *Integrated Photonics*. Wiley-Blackwell, 2003.

[48] T. Shoji, T. Tsuchizawa, T. Watanabe, K. Yamada, and H. Morita, "Low loss mode size converter from 0.3 μm square An Si wire waveguides to singlemode fibres," *Electronics Letters*, vol. 38, pp. 1669–1670(1), December 2002.

[49] D. Taillaert, W. Bogaerts, P. Bienstman, T. F. Krauss, P. V. Daele, I. Moerman, S. Verstuyft, K. D. Mesel, and R. Baets, "An out-of-plane grating coupler for efficient butt-coupling between compact planar waveguides and single-mode fibers," *IEEE Journal of Quantum Electronics*, vol. 38, pp. 949–955, Jul 2002.

[50] G. T. Reed and A. P. Knights, *Silicon Photonics*. John Wiley & Sons, Ltd, 2005.

[51] E. A. J. Marcatili, "Dielectric rectangular waveguide and directional coupler for integrated optics," *The Bell System Technical Journal*, vol. 48, pp. 2071–2102, Sept 1969.

[52] L. B. Soldano and E. C. M. Pennings, "Optical multi-mode interference devices based on self-imaging: principles and applications," *Journal of Lightwave Technology*, vol. 13, pp. 615–627, Apr 1995.

[53] P. P. Absil, P. De Heyn, H. Chen, P. Verheyen, G. Lepage, M. Pantouvaki, J. De Coster, A. Khanna, Y. Drissi, D. Van Thourhout, and J. Van Campenhout, "Imec iSiPP25G silicon photonics: a robust CMOS-based photonics technology platform," 2015.

[54] S. Sze and K. Ng, *Physics of Semiconductor Devices*. Wiley, 2006.

[55] P. Verheyen, M. Pantouvaki, P. D. Heyn, H. Chen, G. Lepage, J. D. Coster, P. Dumon, A. Masood, D. V. Thourhout, R. Baets, W. Bogaerts, P. Absil, and J. V. Campenhout, "Highly uniform 28 Gb/s Si photonics platform for high-density, low-power WDM optical interconnects," in *Advanced Photonics for Communications*, p. IW3A.4, Optical Society of America, 2014.

[56] M. Smit et al., "An introduction to InP-based generic integration technology," *Semiconductor Science and Technology*, vol. 29, no. 8, p. 083001, 2014.

[57] J. Bertrand and P. Bertrand, "A tomographic approach to Wigner's function," *Foundations of Physics*, vol. 17, pp. 397–405, April 1987.

[58] U. Leonhardt, *Measuring the Quantum State of Light*. Cambridge University Press, 1997.

[59] A. I. Lvovsky, H. Hansen, T. Aichele, O. Benson, J. Mlynek, and S. Schiller, "Quantum state reconstruction of the single-photon fock state," *Physical Review Letters*, vol. 87, p. 050402, Jul 2001.

[60] A. I. Lvovsky, "Iterative maximum-likelihood reconstruction in quantum homodyne tomography," *Journal of Optics B: Quantum and Semiclassical Optics*, vol. 6, no. 6, p. S556, 2004.

[61] K. Konishi and G. Paffuti, *Quantum mechanics: a new introduction*. Oxford University Press, 2009.

[62] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani, "Quantum randomness extraction for various levels of characterization of the devices," *Journal of Physics A: Mathematical and Theoretical*, vol. 47, no. 42, p. 424028, 2014.

[63] S. Pironio, A. Acin, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroei, "Random numbers certified by Bell's theorem," *Nature*, vol. 464, pp. 1021–1024, April 2010.

[64] Y. Liu et al., "Device-independent quantum random number generator," *Nature*, vol. 562, pp. 548–551, Sept. 2018.

[65] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," *Physical Review A*, vol. 87, p. 062327, Jun 2013.

[66] A. D. Semenov, G. N. Gol'tsman, and A. A. Korneev, "Quantum detection by current carrying superconducting film," *Physica C: Superconductivity*, vol. 351, no. 4, pp. 349 – 356, 2001.

[67] B. Chor and O. Goldreich, "Unbiased bits from sources of weak randomness and probabilistic communication complexity," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 230–261, 1988.

[68] D. Zuckerman, "General weak random sources," in *Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science*, pp. 534–543 vol.2, Oct 1990.

[69] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," *Phys. Rev. Lett.*, vol. 103, p. 024102, Jul 2009.

[70] X. Zhang, Y. Nie, H. Liang, and J. Zhang, "FPGA implementation of Toeplitz hashing extractor for real time post-processing of raw random numbers," in *2016 IEEE-NPSS Real Time Conference (RT)*, pp. 1–5, June 2016.

[71] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *National Institute of Technology*, April 2010.

[72] H. M. J. Hung, R. T. O'Neill, P. Bauer, and K. Kohne, "The behavior of the p-value when the alternative hypothesis is true," *Biometrics*, vol. 53, no. 1, pp. 11–22, 1997.

[73] L. Wasserman, *All of Statistics: A Concise Course in Statistical Inference*. Springer Texts in Statistics, Springer, 2004.

[74] F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. F. Matthews, "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers," *Quantum Science and Technology*, vol. 3, no. 2, p. 025003, 2018.

[75] E. Bimbard, N. Jain, A. MacRae, and A. I. Lvovsky, "Quantum-optical state engineering up to the two-photon level," *Nature Photonics*, vol. 4, pp. 243–247, April 2010.

[76] S. Yokoyama, R. Ukai, S. C. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J.-i. Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa, "Ultra-large-scale continuous-variable cluster states multiplexed in the time domain," *Nature Photonics*, vol. 7, p. 982, Dec 2013.

[77] G. Masada, K. Miyata, A. Politi, T. Hashimoto, J. L. O'brien, and F. Akira, "Continuous-variable entanglement on a chip," *Nature Photonics*, vol. 9, pp. 316–319, May 2015.

[78] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, "Detection of 15 dB squeezed states of light and their application for the absolute calibration of photoelectric quantum efficiency," *Physical Review Letters*, vol. 117, p. 110801, Sep 2016.

[79] S. Ast, M. Mehmet, and R. Schnabel, "High-bandwidth squeezed light at 1550 nm from a compact monolithic PPKTP cavity," *Optics Express*, vol. 21, pp. 13572–13579, Jun 2013.

[80] D. T. Smithey, M. Beck, M. G. Raymer, and A. Faridani, "Measurement of the Wigner distribution and the density matrix of a light mode using optical homodyne tomography: Application to squeezed states and the vacuum," *Physical Review Letters*, vol. 70, pp. 1244–1247, Mar 1993.

[81] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, "Unconditional quantum teleportation," *Science*, vol. 282, no. 5389, pp. 706–709, 1998.

[82] S. Lloyd and S. L. Braunstein, "Quantum computation over continuous variables," *Physical Review Letters*, vol. 82, pp. 1784–1787, Feb 1999.

[83] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7 – 11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[84] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, vol. 421, pp. 238–241, jan 2003.

[85] A. Zavatta, S. Viciani, and M. Bellini, "Quantum-to-classical transition with single-photon-added coherent states of light," *Science*, vol. 306, no. 5696, pp. 660–662, 2004.

[86] A. Ourjoumtsev, H. Jeong, Tualle-Brouri, and P. Grangier, "Generation of optical Schrödinger cats from photon number states," *Nature*, vol. 448, pp. 784–786, August 2007.

[87] R. Kumar, E. Barrios, A. MacRae, E. Cairns, E. Huntington, and A. Lvovsky, "Versatile wideband balanced detector for quantum optical homodyne tomography," *Optics Communications*, vol. 285, no. 24, pp. 5259–5267, 2012.

[88] J. Appel, D. Hoffman, E. Figueroa, and A. I. Lvovsky, "Electronic noise in optical homodyne tomography," *Physical Review A*, vol. 75, no. 3, p. 035802, 2007.

[89] M. Esposito, F. Randi, K. Titimbo, G. Kourousias, A. Curri, R. Floreanini, F. Parmigiani, D. Fausti, K. Zimmermann, and F. Benatti, "Quantum interferences reconstruction with low homodyne detection efficiency," *EPJ Quantum Technology*, vol. 3, no. 1, pp. 1–17, 2016.

[90] M. Esposito, F. Benatti, R. Floreanini, S. Olivares, F. Randi, K. Titimbo, M. Pividori, F. Novelli, F. Cilento, F. Parmigiani, and D. Fausti, "Pulsed homodyne Gaussian quantum tomography with low detection efficiency," *New Journal of Physics*, vol. 16, no. 4, p. 043004, 2014.

[91] C. M. Wilkes, X. Qiang, J. Wang, R. Santagati, S. Paesani, X. Zhou, D. A. B. Miller, G. D. Marshall, M. G. Thompson, and J. L. O'Brien, "60 dB high–extinction auto-configured Mach–Zehnder interferometer," *Optics Letters*, vol. 41, pp. 5318–5321, Nov 2016.

[92] J. Yang, J. Liu, Q. Su, Z. Li, F. Fan, B. Xu, and H. Guo, "5.4 Gbps real time quantum random number generator with simple implementation," *Optics Express*, vol. 24, pp. 27475–27481, Nov 2016.

[93] `http://csrc.nist.gov/groups/ST/toolkit/rng/`. Accessed: May 2016.

[94] M. W. Mitchell, C. Abellan, and W. Amaya, "Strong experimental guarantees in ultrafast quantum random number generation," *Phys. Rev. A*, vol. 91, p. 012314, Jan 2015.

[95] "Wideband, ultra-low noise, voltage-feedback OPERATIONAL AMPLIFIER with shutdown." `http://www.ti.com/lit/ds/symlink/opa847.pdf`. Accessed: November 2014.

[96] D. Huang, J. Fang, C. Wang, P. Huang, and G.-H. Zeng, "A 300-MHz bandwidth balanced homodyne detector for continuous variable quantum key distribution," *Chinese Physics Letters*, vol. 30, no. 11, p. 114209, 2013.

[97] X. Zhang, Y. Zhang, Z. Li, S. Yu, and H. Guo, "1.2 GHz balanced homodyne detector for continuous-variable quantum information technology." arXiv:1806.09393 [physics.ins-det], 2018.

[98] F. Raffaelli, P. Sibson, J. E. Kennard, D. H. Mahler, M. G. Thompson, and J. C. F. Matthews, "Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip," *Optics Express*, vol. 26, pp. 19730–19741, Aug 2018.

[99] K. Petermann, *Laser Diode Modulation and Noise*. Kluwer Academic Publishers, 1988.

[100] C. Henry, "Theory of the linewidth of semiconductor lasers," *IEEE Journal of Quantum Electronics*, vol. QE-18, no. 2, pp. 259–264, 1982.

[101] K. Vahala and A. Yariv, "Occupation fluctuation noise: A fundamental source of linewidth broadening in semiconductor lasers," *Applied Physics Letters*, vol. 43, no. 2, pp. 140–142, 1983.

[102] F. Gravetter and L. Wallnau, *Statistics for the Behavioral Sciences*. Available Titles Aplia Series, Wadsworth, 2009.

[103] K. Kaur, A. Subramanian, P. Cardile, R. Verplancke, J. V. Kerrebrouck, S. Spiga, R. Meyer, J. Bauwelinck, R. Baets, and G. V. Steenberge, "Flip-chip assembly of VCSELs to silicon grating couplers via laser fabricated SU8 prisms," *Optics Express*, vol. 23, pp. 28264–28270, Nov 2015.

[104] C. Gerry and P. Knight, *Introductory Quantum Optics*. Cambridge University Press, 2005.

[105] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-based quantum key distribution," *Nature Communications*, vol. 8, p. 13984, feb 2017.

[106] M. Lobino, D. Korystov, C. Kupchak, E. Figueroa, B. C. Sanders, and A. I. Lvovsky, "Complete characterization of quantum-optical processes," *Science*, vol. 322, no. 5901, pp. 563–566, 2008.

[107] S. Rahimi-Keshari, A. Scherer, A. Mann, A. T. Rezakhani, A. I. Lvovsky, and B. C. Sanders, "Quantum process tomography with coherent states," *New Journal of Physics*, vol. 13, no. 1, p. 013006, 2011.

[108] I. A. Fedorov, A. K. Fedorov, Y. V. Kurochkin, and A. I. Lvovsky, "Tomography of a multimode quantum black box," *New Journal of Physics*, vol. 17, no. 4, p. 043063, 2015.

[109] A. Beling, H. G. Bach, D. Schmidt, G. G. Mekonnen, M. Rohde, L. Molle, H. Ehlers, and A. Umbach, "High-speed balanced photodetector module with 20 dB broadband common-mode rejection ratio," in *OFC 2003 Optical Fiber Communications Conference, 2003*, pp. 339–340 vol.1, March 2003.

[110] H. . Bach, A. Beling, G. G. Mekonnen, R. Kunkel, D. Schmidt, W. Ebert, A. Seeger, M. Stollberg, and W. Schlaak, "InP-based waveguide-integrated photodetector with 100-GHz bandwidth," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 10, pp. 668–672, July 2004.

[111] R. Kaiser, D. Trommer, F. Fidorra, H. Heidrich, S. Malchow, D. Franke, W. Passenberg, W. Rehbein, H. Schroeter-Janssen, R. Stenzel, and G. Unterborsch, "Monolithically integrated polarisation diversity heterodyne receivers on GaInAsP/InP," *Electronics Letters*, vol. 30, pp. 1446–1447, Aug 1994.

[112] "LTC6268-10 - 4 GHz ultra-low bias current FET input op amp." `http://www.linear.com/product/LTC6268-10`. Accessed: June 2015.

[113] A. V. Masalov, A. Kuzhamuratov, and A. I. Lvovsky, "Noise spectra in balanced optical detectors based on transimpedance amplifiers," *Review of Scientific Instruments*, vol. 88, no. 11, p. 113109, 2017.

[114] J. R. Andrews, "Broadband coaxial bias tees." Application note AN-1e, November 2000.

[115] G. Johnson, "Bias tee." `http://wb9jps.com/Gary_Johnson/Bias_Tee.html`. Accessed: July 2018.

[116] P. Horowitz and W. Hill, *The Art of Electronics*. Cambridge University Press, 2015.

[117] A. Johnson and M. Graham, *High-Speed Digital Design - A Handbook for Black Magic*. Prentice-Hall, 1993.

[118] "MAX3277 - Low-noise, fibre channel transimpedance amplifiers." `https://www.maximintegrated.com/en/products/comms/optical-communications/MAX3277.html`. Accessed: September 2018.

[119] "HMC799 - DC - 700 MHz, 10 kOhm transimpedance amplifier SMT." `http://www.analog.com/en/products/hmc799.html`. Accessed: September 2018.

[120] "OPA858 - 5.5 GHz gain bandwidth product, decompensated transimpedance amplifier with FET input." `http://www.ti.com/product/OPA858`. Accessed: September 2018.

[121] "OPA855 - 8 GHz gain bandwidth product, decompensated transimpedance amplifier with bipolar input." `http://www.ti.com/product/OPA855`. Accessed: September 2018.

[122] "LT6409 - 10 GHz GBW, 1.1 nv/$\sqrt{Hz}$ differential amplifier/ADC driver." `http://www.analog.com/en/products/ltc6409.html`. Accessed: September 2018.